A framework for quantum-secure device-independent randomness expansion

Peter J. Brown*, Sammy Ragy†, and Roger Colbeck‡

Department of Mathematics, University of York, Heslington, York YO10 5DD, United Kingdom

Thursday 26th September, 2019

Abstract

A device-independent randomness expansion protocol aims to take an initial random seed and generate a longer one without relying on details of how the devices operate for security. A large amount of work to date has focussed on a particular protocol based on spot-checking devices using the CHSH inequality. Here we show how to derive randomness expansion rates for a wide range of protocols, with security against a quantum adversary. Our technique uses semidefinite programming and a recent improvement of the entropy accumulation theorem. To support the work and facilitate its use, we provide code that can generate lower bounds on the amount of randomness that can be output based on the measured quantities in the protocol. As an application, we give a protocol that robustly generates up to two bits of randomness per entangled qubit pair, which is twice that established in existing analyses of the spot-checking CHSH protocol in the low noise regime.

1 Introduction

Random numbers are an essential resource in the information processing era, finding applications in gaming, simulations and cryptography. Cryptographic protocols are frequently built upon an assumption of access to a private random seed. Using poor-quality randomness can be fatal to the security of the protocol (see, e.g., [1]). Thus, in order to adhere to these standard protocol assumptions, it is imperative that we are able to certify the generation of private random numbers.

The intrinsic randomness of quantum theory provides a natural mechanism with which we can generate random numbers: a simple source of perfectly random bits could be a device that prepares a σ_x eigenstate and then measures σ_z. However, the use of such a source comes with a significant caveat: the internal mechanisms of the preparation and measurement devices must be well-characterized and kept stable throughout their use. Any mismatch between the characterization and how the device operates in practice may be an exploitable weakness in the hands of a smart enough adversary; such mismatches have been used to compromise commercially available quantum key distribution (QKD) systems (see e.g., [2]).

While weaknesses caused by mismatches may be mitigated by increasingly detailed descriptions of the quantum devices, generating such descriptions rapidly becomes unwieldy and remaining vulnerabilities can be difficult to detect. This is reminiscent of the situation in modern software engineering where security flaws are frequently discovered and patched. Fixing hardware vulnerabilities, such as those exploited in the aforementioned QKD attacks, can be more difficult logistically and economically.

Fortunately, quantum theory provides a means to address this problem. Going back to [3] and using an important insight of [4], device-independent quantum cryptography establishes security independently of the devices involved within a protocol, relying only on the validity of quantum theory and the imposition of certain no-signalling constraints between devices. Security is subsequently verified through the observation

*peter.brown@york.ac.uk
†sammy.ragy@york.ac.uk
‡roger.colbeck@york.ac.uk

of non-local output statistics, which in turn act as witnesses to the inner workings of the devices. Limiting the number of initial assumptions greatly reduces the threat of side-channel attacks.

In this work we focus on the task of randomness expansion: a procedure wherein one attempts to transform a short private seed into a much larger (still private) source of uniform random bits. Randomness expansion in a device-independent setting was proposed in [5, 6] with further development and experimental testing following shortly after [7]. Subsequent work provided security proofs against classical adversaries [8, 9]. Security against quantum adversaries—who may share entanglement with the internal state of the device—came later [10–12], progressively increasing in noise-tolerance and generality, with the recently introduced entropy accumulation theorem (EAT) [13, 23], on which our work is based, providing asymptotically optimal rates [14, 15]. A new proof technique that is also asymptotically optimal has recently appeared [16].

In [14] the EAT was applied to the task of randomness expansion and a general entropy accumulation procedure was detailed. The security of the resulting randomness expansion protocol relies on the construction of a randomness bounding function (known as a min-tradeoff function) that characterizes the average entropy gain during the protocol. Unfortunately, the analysis in [14] applies only to protocols based on the CHSH inequality, and relies on some analytic steps that do not directly generalize to arbitrary protocols[1]. However, as was also noted in [14], one could look to use the device-independent guessing probability (DIGP) [20–22] in conjunction with the semidefinite hierarchy [18, 19] to obtain computational constructions of the required min-tradeoff functions.

Here we detail a precise method for combining these semidefinite programming tools with the EAT to construct min-tradeoff functions. We then apply this construction to the task of randomness expansion to prove security of protocols based upon arbitrary nonlocal games. This includes protocols with arbitrary (but finite) numbers of inputs-outputs, as well as protocols based upon multiple Bell-inequalities [17]. It is worth noting that this construction could also be readily extended to multipartite scenarios although we do not discuss these in this work. Moreover, as this computational method takes the form of a semidefinite program these constructions are both computationally efficient and reliable, although at the cost of producing potentially suboptimal bounds. To accompany this work, we provide a code package (available at [24]) for the construction and analysis of these randomness expansion protocols.

In more detail, we give a template protocol, Protocol QRE, from which a user can develop their randomness expansion protocol. Given certain parameters chosen by a user, e.g., time constraints, choice of non-locality tests and security tolerances, the projected randomness expansion rates to be calculated. If these rates are unsatisfactory, then modifications to the protocol's design can be made and the rates recalculated. As the computations can be done with a computationally efficient procedure, the user can optimize their protocol parameters to best fit their experimental setup. Once a choice of experimental design has been made, the resulting randomness expansion procedure can be performed. Subject to the protocol not aborting, this gives a certifiably private random bit-string.

We apply our technique to several example protocols. In particular, we look at randomness expansion using the complete empirical distribution as well as a simple extension of the CHSH protocol, showing noise-tolerant rates of up to two bits per entangled qubit pair, secure against quantum adversaries. Although means of generating two bits of randomness per entangled qubit pair have been considered before [25] to the best of our knowledge our work is the first to present a full protocol and prove that this rate can be robustly achieved taking into account finite statistics. The nonlocal game we use for this is related to that in [25]. We also compare the achievable rates for these protocols to the protocol presented in [14] which is based upon a direct von Neumann entropy bound. Our comparison demonstrates that some of the protocols from the framework are capable of achieving higher rates than the protocol of [14], in both the low and high noise regimes. Improved rates in the high noise regime are of particular importance when considering current experimental implementations, because of the difficulty of significantly violating the CHSH inequality while closing the detection loophole [26–28]. Additionally, we include in the appendices a full non-asymptotic account of input randomness necessary for running the protocols.

The paper is structured as follows: in Sec. 2 we introduce the material relevant for our construction. In Sec. 3 we detail the various components of our framework and present the template protocol with full security statements and proofs. We provide examples of several randomness expansion protocols built within our framework in Sec. 4 before concluding with some open problems in Sec. 5.

[1] In particular, simplifications that arise due to the two party, two input, two output scenario being reducible to qubits.

2 Preliminaries

2.1 General notation

Throughout this work, the calligraphic symbols $\mathcal{A}$, $\mathcal{B}$, $\mathcal{X}$ and $\mathcal{Y}$ denote finite alphabets and we use the notational shorthand $\mathcal{AB}$ to denote the Cartesian product alphabet $\mathcal{A} \times \mathcal{B}$. We refer to a *behaviour* (or *strategy*) on these alphabets as some conditional probability distribution, $(p(a,b|x,y))_{ab|xy}$ with $abxy \in \mathcal{ABXY}$, which we view as a vector $\boldsymbol{p} \in \mathbb{R}^{|\mathcal{ABXY}|}$. That is, by denoting the set of canonical bases vectors of $\mathbb{R}^{|\mathcal{ABXY}|}$ by $\{\mathbf{e}_{ab|xy}\}_{abxy}$, we write $\boldsymbol{p} = \sum_{abxy} p(a,b|x,y)\mathbf{e}_{ab|xy}$. We make the distinction between the vector and its elements through the use of boldface, i.e., $p(a,b|x,y) = \boldsymbol{p} \cdot \mathbf{e}_{ab|xy}$. Throughout this work we assume that all conditional distributions obey the no-signalling constraints that $\sum_{a\in\mathcal{A}} p(a,b|x,y)$ is independent of x and hence can be written $p(b|y)$ and similarly $\sum_{b\in\mathcal{B}} p(a,b|x,y) = p(a|x)$. We denote the set of all no-signalling behaviours by $\mathcal{P}_{\mathcal{AB}|\mathcal{XY}} \subset \mathbb{R}^{|\mathcal{ABXY}|}$. Given an alphabet $\mathcal{C}$ we denote the set of all distributions over $\mathcal{C}$ by $\mathcal{P}_{\mathcal{C}}$, and given a sequence $\mathbf{C} = (c_i)_{i=1}^n$, with $c_i \in \mathcal{C}$ for each $i = 1, \ldots, n$, we denote the frequency distribution induced by $\mathbf{C}$ by

$$F_{\mathbf{C}}(x) = \frac{\sum_{i=1}^n \delta_{xc_i}}{n}, \tag{1}$$

where δ_{ab} is the Kronecker delta on the set $\mathcal{C}$.

We use the symbol $\mathcal{H}$ to denote a Hilbert space, subscripting with system labels when helpful. For a system E, we denote the set of positive semidefinite operators with unit trace acting on $\mathcal{H}_E$ by $\mathcal{S}(E)$ and its subnormalized extension (i.e., the set that arises when the trace is restricted to be in the interval $[0,1]$) by $\tilde{\mathcal{S}}(E)$ (we extend the use of tildes to other sets to denote their subnormalized extensions). We refer to a state $\rho_{XE} \in \mathcal{S}(XE)$ as a *classical-quantum state* (cq-state) on the joint system XE if it can be written in the form $\rho_{XE} = \sum_x p(x) \left|x\right\rangle\!\left\langle x\right| \otimes \rho_E^x$ where $\{\left|x\right\rangle\}_x$ is a set of orthonormal vectors in $\mathcal{H}_X$. Letting $\Omega \subseteq \mathcal{X}$ be an event on the alphabet $\mathcal{X}$, we define the *conditional state* (conditioned on the event Ω) by

$$\rho_{XE|\Omega} = \frac{1}{\Pr[\Omega]} \sum_{x\in\Omega} p(x) \left|x\right\rangle\!\left\langle x\right| \otimes \rho_E^x. \tag{2}$$

We denote the identity operator of a system E by $\mathbb{1}_E$. We write the natural logarithm as $\ln(\cdot)$ and the logarithm base 2 as $\log(\cdot)$. The function $\mathrm{sgn} : \mathbb{R} \to \{-1, 0, 1\}$ is the sign function, mapping all positive numbers to 1, negative numbers to -1 and 0 to 0.

We say that a behaviour $\boldsymbol{p} \in \mathcal{P}_{\mathcal{AB}|\mathcal{XY}}$ is *quantum* if its elements can be written in the form $p(a,b|x,y) = \mathrm{Tr}\left[\rho_{AB}(N_{a|x} \otimes M_{b|y})\right]$ where $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\{\{N_{a|x}\}_{a\in\mathcal{A}}\}_{x\in\mathcal{X}}$, $\{\{M_{b|y}\}_{b\in\mathcal{B}}\}_{y\in\mathcal{Y}}$ are sets of POVMs; we denote the set of all quantum behaviours by $\mathcal{Q}$. Additionally, we use $\tilde{\mathcal{Q}}$ to denote the subnormalized extension of this set.

Note that randomness expansion is a single-party protocol; there is one user who wishes to expand an initial private random string. However, that user may work with a bipartite setup in which they use two devices that are prevented from signalling to one another; in such a case we sometimes refer to Alice and Bob as the users of each device. Note though that, unlike in QKD, Alice and Bob are agents of the same party and are within the same laboratory. There may also be a dishonest party, Eve, trying to gain information about the random outputs.

2.2 Entropies and SDPs

The von Neumann entropy of $\rho \in \mathcal{S}(A)$ is

$$H(A)_\rho := -\mathrm{Tr}\left[\rho \log(\rho)\right]. \tag{3}$$

For a bipartite state $\rho_{AE} \in \mathcal{S}(AE)$, we use the notation ρ_E for $\mathrm{Tr}_A\left[\rho_{AE}\right]$ and define the conditional von Neumann entropy of system A given system E when the joint system is in state ρ_{AE} by

$$H(A|E)_\rho := H(AE)_\rho - H(E)_\rho. \tag{4}$$

In addition, for a tripartite system $\rho_{ABE} \in \mathcal{S}(ABE)$, the conditional mutual information between A and B given E is defined by

$$I(A:B|E)_\rho = H(A|BE)_\rho - H(A|E)_\rho.$$

We drop the state subscript whenever the state is clear from the context.

In this work it is useful to consider the conditional min-entropy [30] in its operational formulation [22]. Given a cq-state $\rho_{XE} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_E^x$, the maximum probability with which an agent holding system E can guess the outcome of a measurement on X is

$$p_{\text{guess}}(X|E) := \max_{\{M_x\}_x} \sum_x p(x) \text{Tr}\left[M_x \rho_E^x\right], \tag{5}$$

where the maximum is taken over all POVMs $\{M_x\}_x$ on system E. Using this we can define the min-entropy of a classical system given quantum side information as

$$H_{\min}(X|E) := -\log\left(p_{\text{guess}}(X|E)\right). \tag{6}$$

The final entropic quantity we consider is the *ϵ-smooth min-entropy* [31]. Given some $\epsilon \geq 0$ and $\rho_{XE} \in \mathcal{S}(XE)$, the ϵ-smooth min-entropy $H_{\min}^{\epsilon}$ is defined as the supremum of the min-entropy over all states ϵ-close to ρ_{XE},

$$H_{\min}^{\epsilon}(X|E)_{\rho} := \sup_{\rho' \in B_{\epsilon}(\rho)} H_{\min}(X|E)_{\rho'}, \tag{7}$$

where $B_{\epsilon}(\rho)$ is the ϵ-ball centred at ρ defined with respect to the purified trace distance [32]. For a thorough overview of smooth entropies and their properties we refer the reader to [33].

In the device-independent scenario we do not know the quantum states or measurements being performed. Instead, our entire knowledge about these must be inferred from the observed input-output behaviour of the devices used. In particular, observing correlations that violate a Bell inequality provides a coarse-grained characterization of the underlying system. In a device-independent protocol, the idea is to use only this to infer bounds on particular system quantities, e.g., the randomness present in the outputs. As formulated above, the guessing probability (5) is not a device-independent quantity because its computation requires knowing ρ_E^x. However, the guessing probability can be reformulated in a device-independent way [17,20,21,34] as we now explain.

Consider a tripartite system ρ_{ABE} shared between two devices in the user's lab and Eve. Because we are assuming an adversary limited by quantum theory, we can suppose that, upon receiving some inputs $(x, y) \in \mathcal{X}\mathcal{Y}$, the devices work by performing measurements $\{E_{a|x}\}_a$ and $\{F_{b|y}\}_b$ respectively, which give rise to some probability distribution $\boldsymbol{p} \in \mathcal{Q}_{\mathcal{A}\mathcal{B}|xy}$, and overall state

$$\sigma_{ABE}^{x,y} = \sum_{ab} |a\rangle\langle a| \otimes |b\rangle\langle b| \otimes \tilde{\rho}_E^{abxy},$$

where $\text{Tr}_{AB}\left[(E_{a|x} \otimes F_{b|y} \otimes \mathbb{1}_E)\rho_{ABE}\right] = \tilde{\rho}_E^{abxy}$, and $p(a, b|x, y) = \text{Tr}\left[\tilde{\rho}_E^{abxy}\right]$. Note that the user of the protocol is not aware of what the devices are doing.

Consider the best strategy for Eve to guess the value of AB using her system E. She can perform a measurement on her system to try to distinguish $\{\rho_E^{abxy}\}_{ab}$ (occurring with probability $p(a, b|x, y)$). Denoting Eve's POVM $\{M_c\}_c$ with outcomes in one-to-one correspondence with the values AB can take (say c_{ab} being the value corresponding to a best guess of $AB = (a, b)$)[2], then given some values of a, b, x and y, Eve's outcomes are distributed as $p(c_{a'b'}|a, b, x, y) = \text{Tr}\left[M_{c_{a'b'}} \rho_E^{abxy}\right]$, and her probability of guessing correctly is $p(c_{ab}|a, b, x, y) = \text{Tr}\left[M_{c_{ab}} \rho_E^{abxy}\right]$. Hence, the overall probability of guessing AB correctly given E and $XY = (x, y)$ for the quantum realisation of the statistics, $q = \{\rho_{ABE}, \{E_{a|x}\}, \{F_{b|y}\}\}$, is

$$\begin{aligned} p_{\text{guess}}(AB|x, y, E, q) &= \sup_{\{M_c\}_c} \sum_{ab} \text{Tr}\left[(E_{a|x} \otimes F_{b|y} \otimes M_{c_{ab}})\rho_{ABE}\right] \\ &= \sup_{\{M_c\}_c} \sum_{ab} p(a, b, c_{ab}|x, y, q) \\ &= \sup_{\{M_c\}_c} \sum_{ab} p(c_{ab}|a, b, x, y, q) p(a, b|x, y, q). \end{aligned}$$

[2]Without loss of generality we can assume Eve's measurement has as many outcomes as what she is trying to guess.

Note that the guessing probability depends on the inputs x, y. In the protocols we consider later, there will only be one pair of inputs for which Eve is interested in guessing the outputs. We denote these inputs by $\tilde{x}$ and $\tilde{y}$.

In the device-independent scenario, Eve can also optimize over all quantum states and measurements that could be used by the devices. However, she wants to do so while restricting the devices to obey certain relations which depend on the protocol (for example, the CHSH violation that could be observed by the user). For the moment, without specifying these relations precisely, call the set of quantum states and measurements obeying these relations $\mathcal{R}$. Hence, we seek

$$p_{\text{guess}}(AB|\tilde{x},\tilde{y},E) = \sup_{q\in\mathcal{R},\{M_c\}_c} \sum_{ab} p(a,b|\tilde{x},\tilde{y},q)p(c_{ab}|a,b,\tilde{x},\tilde{y},q)\,.$$

Because Eve's measurement commutes with those of the devices, due to no signalling we can use Bayes' rule to rewrite the optimization as[3]

$$\sup_{q\in\mathcal{R},\{M_c\}_c} \sum_{ab} p(c_{ab}|\tilde{x},\tilde{y},q)p(a,b|c_{ab},\tilde{x},\tilde{y},q)\,.$$

With this rewriting it is evident that we can think about Eve's strategy as follows: Eve randomly chooses a value of C and then prepares the device according to that choice, i.e., trying to bias A, B towards the values a, b corresponding to the chosen c.

We can hence write

$$p_{\text{guess}}(AB|\tilde{x},\tilde{y},E) = \sup_{\{\boldsymbol{p}_c\}_c} \sum_{ab} \Pr\left[C=c_{ab}\right] p_{c_{ab}}(a,b|\tilde{x},\tilde{y},q)\,,$$

where $\sum_c p(c)\boldsymbol{p}_c$ satisfies some relations (equivalent to the restriction to the set $\mathcal{R}$) and $\boldsymbol{p}_c \in \mathcal{Q}_{\mathcal{AB}|\mathcal{XY}}$ for each c. Provided the relations satisfied are linear, which we will henceforth assume, they can be expressed as a matrix equation $\boldsymbol{W}\boldsymbol{p} = \boldsymbol{\omega}$ and the whole optimization is a conic program (the set of un-normalized quantum-realisable distributions forms a convex cone). By writing $\Pr\left[C=c\right]\boldsymbol{p}_c$ as the subnormalized distribution $\tilde{\boldsymbol{p}}_c$ the problem can be expressed as

$$\begin{aligned} \sup_{\{\tilde{\boldsymbol{p}}_c\}_c} \quad & \sum_{ab} \tilde{p}_{c_{ab}}(a,b|\tilde{x},\tilde{y}) \\ \text{subj. to} \quad & \sum_c \boldsymbol{W}\tilde{\boldsymbol{p}}_c = \boldsymbol{\omega} \\ & \tilde{\boldsymbol{p}}_c \in \tilde{\mathcal{Q}}_{\mathcal{AB}|\mathcal{XY}} \quad \forall\, c\,. \end{aligned} \tag{8}$$

Note that the normalisation condition, $\sum_{abc}\tilde{p}_c(a,b|\tilde{x},\tilde{y}) = 1$, is assumed to be contained within (or a consequence of) the conditions imposed by $\boldsymbol{W}$. For the particular sets of conditions that we impose later, normalization always follows.

Optimizing over the set of quantum correlations is a difficult problem, in part because the dimension of the quantum system achieving the optimum could be arbitrarily large. Because of this, we consider a computationally tractable relaxation of the problem, by instead optimizing over distributions within some level of the semidefinite hierarchy [18, 19]. We denote the k^{th} level by $\tilde{\mathcal{Q}}^{(k)}$. This relaxation of the problem takes the form of a semidefinite program that can be solved in an efficient manner, at the expense of possibly not obtaining the same optimum value. The corresponding relaxed program is

$$\begin{aligned} p^{(k)}_{\text{guess}}(\boldsymbol{\omega}) := \sup_{\{\tilde{\boldsymbol{p}}_c\}_c} \quad & \sum_{ab} \tilde{p}_{c_{ab}}(a,b|\tilde{x},\tilde{y}) \\ \text{subj. to} \quad & \sum_c \boldsymbol{W}\tilde{\boldsymbol{p}}_c = \boldsymbol{\omega} \\ & \tilde{\boldsymbol{p}}_c \in \tilde{\mathcal{Q}}^{(k)} \quad \forall\, c\,. \end{aligned} \tag{9}$$

[3]This rewriting makes sense provided no information leaks to Eve during the protocol, which is reasonable for randomness expansion since it takes place in one secure lab.

This program has a dual. In Appendix D we show that there is an alternative program with the same properties[4] as the standard dual. To specify this, we define the set $\mathcal{V}^{(k)}$ of *valid constraint vectors at level k* by the set of vectors $\boldsymbol{\nu}$ for which there exists $\boldsymbol{p} \in \mathcal{Q}^{(k)}$ such that $\boldsymbol{W}\boldsymbol{p} = \boldsymbol{\nu}$.

The alternative dual then takes the form

$$\begin{aligned} d^{(k)}_{\text{guess}}(\boldsymbol{\omega}) := \inf_{\boldsymbol{\lambda}} \quad & \boldsymbol{\lambda} \cdot \boldsymbol{\omega} \\ \text{subj. to} \quad & p^{(k)}_{\text{guess}}(\boldsymbol{\nu}) \leq \boldsymbol{\lambda} \cdot \boldsymbol{\nu}, \quad \forall\, \boldsymbol{\nu} \in \mathcal{V}^{(k)}, \end{aligned} \tag{10}$$

with $\boldsymbol{\lambda} \in \mathbb{R}^{\|\boldsymbol{\omega}\|_0}$. Since the NPA hierarchy forms a sequence of outer approximations to the set of quantum correlations, $\mathcal{Q}_1 \supseteq \mathcal{Q}_2 \supseteq \cdots \supseteq \mathcal{Q}$, the relaxed guessing probability provides an upper bound on the true guessing probability, i.e., $p_{\text{guess}}(\boldsymbol{\omega}) \leq p^{(k)}_{\text{guess}}(\boldsymbol{\omega})$. Combined with (6), one can use the relaxed programs to compute valid device-independent lower bounds on $H_{\min}$.

Programs (9) and (10) are parameterized by a vector $\boldsymbol{\omega}$. We denote a feasible point of the dual program parameterized by $\boldsymbol{\omega}$ by $\boldsymbol{\lambda}_{\boldsymbol{\omega}}$. Note that for our later analysis we only need $\boldsymbol{\lambda}_{\boldsymbol{\omega}}$ to be a feasible point of the dual program, we do not require it to be optimal.[5]

2.3 Devices and nonlocal games

Device-independent protocols involve a series of interactions with some *untrusted devices*. A *device* $\mathcal{D}$ refers to some physical system that receives classical inputs and produces classical outputs. Furthermore, we say that $\mathcal{D}$ is *untrusted* if the mechanism by which $\mathcal{D}$ produces the outputs from the inputs need not be characterized. During the protocol, the user interacts with their untrusted devices within the following scenario:[6]

1. The protocol is performed within a secure lab from which information can be prevented from leaking.
2. This lab can be partitioned into disconnected sites (one controlled by Alice and one by Bob).
3. The user can send information freely between these sites without being overheard, while at the same time, they can prevent unwanted information transfer between the sites.[7]
4. The user has two devices to which they can provide inputs (taken from alphabets $\mathcal{X}$ and $\mathcal{Y}$) and receive outputs (from alphabets $\mathcal{A}$ and $\mathcal{B}$).
5. These devices operate according to quantum theory, i.e., $\boldsymbol{p}_{AB|XY} \in \mathcal{Q}_{\mathcal{AB}|\mathcal{XY}}$. Any eavesdropper is also limited by quantum theory[8]. We use $\mathfrak{D}_{ABE}$ to denote the collection of devices (including any held by an eavesdropper) and refer to this as an *untrusted device network*.
6. The user has an initial source of private random numbers and a trusted device for classical information processing.

One of the key advantages of a device-independent protocol is that because no assumptions are made on the inner workings of the devices used, the protocol checks that the devices are working sufficiently well on-the-fly. The protocols hence remain impervious to many side-channel attacks, malfunctioning devices or prior tampering. The idea behind their security is that by testing that the devices exhibit 'nonlocal' correlations, their internal workings are sufficiently restricted to enable the task at hand.

In this work, we formulate the testing of the devices through *nonlocal* games. A nonlocal game is initiated by a referee who sends the two players their own question chosen according to some distribution, μ. The players then respond with their answers chosen from $\mathcal{A}$ and $\mathcal{B}$ respectively. Using the predefined scoring rule V, the referee then announces whether or not they won the game. The game is referred to as *nonlocal*

[4] In particular, the weak duality statement holds.

[5] An optimal choice of $\boldsymbol{\lambda}$ for (10) may not even exist.

[6] One does not have to recreate this scenario exactly in order to perform the protocol. Instead, the given scenario establishes one situation in which the protocol remains secure (see Def. 2.2 for a precise definition of security).

[7] In this work we need to ensure that the user's devices are unable to communicate at certain points of the protocol (when Bell tests are being done), but not at others (e.g., when entanglement is being distributed). However, they should never be allowed to send any information outside the lab after the protocol begins.

[8] In parts of this paper we allow the eavesdropper limited additional power—the bounds will then still apply if the eavesdropper is limited by quantum theory.

because prior to receiving their questions, the players are separated and unable to communicate until they have given their answers. The question sets, answer sets, distribution μ and the scoring rule V are all public knowledge. Moreover, the players are allowed to confer prior to the start of the game.

Definition 2.1: Let $\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}$ and $\mathcal{V}$ be finite sets. A (two-player) *nonlocal game* $\mathcal{G} = (\mu, V)$ (on $\mathcal{ABXY}$) consists of a set of question pairs $(x, y) \in \mathcal{XY}$ chosen according to some probability distribution $\mu : \mathcal{XY} \to [0, 1]$, a set of answer pairs $(a, b) \in \mathcal{AB}$ and a scoring function $V : \mathcal{ABXY} \to \mathcal{V}$. A *strategy* for $\mathcal{G}$ is a conditional distribution $\boldsymbol{p} \in \mathcal{P}_{\mathcal{AB}|\mathcal{XY}}$ defined on the question and answer sets.

Remark 2.1: We will abuse notation and use the symbol $\mathcal{G}$ to refer to both the nonlocal game and the set of possible scores. I.e., we may refer to the players receiving a score $c \in \mathcal{G}$. Furthermore, we denote the number of different scores by $|\mathcal{G}|$.

If the players play $\mathcal{G}$ using the strategy $\boldsymbol{p}$, then this induces a frequency distribution $\boldsymbol{\omega}_{\mathcal{G}}$ over the set of possible scores. That is,

$$\omega_{\mathcal{G}}(c) = \sum_{abxy} \mu(x, y) p(a, b|x, y)\, \delta_{V(a,b,x,y),c} \tag{11}$$

for each $c \in \mathcal{G}$. The expected frequency distribution, $\boldsymbol{\omega}_{\mathcal{G}}$, will be the figure of merit by which we evaluate the performance of our untrusted devices. We denote the set of possible frequency distributions achievable by the agents whilst playing according to quantum strategies by $\mathcal{Q}_{\mathcal{G}}$.

Example 2.1 (Extended CHSH game ($\mathcal{G}_{\text{CHSH}}$))**:** The *extended CHSH game* has appeared already in the device-independent literature in the context of QKD (see, e.g., [35]). It extends the standard CHSH game to include a correlation check between one of Alice's CHSH inputs and an additional input from Bob. It is defined by the question-answer sets $\mathcal{X} = \{0, 1\}$, $\mathcal{Y} = \{0, 1, 2\}$ and $\mathcal{A} = \mathcal{B} = \{0, 1\}$, the scoring set $\mathcal{V} = \{c_{\text{CHSH}}, c_{\text{align}}, 0\}$ and the scoring rule

$$V_{\text{CHSH}}(a, b, x, y) := \begin{cases} c_{\text{CHSH}} & \text{if } x \cdot y = a \oplus b \text{ and } y \neq 2 \\ c_{\text{align}} & \text{if } (x, y) = (0, 2) \text{ and } a \oplus b = 0 \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

The input distribution we consider is defined by $\mu_{\text{CHSH}}(x, y) = \frac{1}{8}$ for $(x, y) \in \{0, 1\}^2$, $\mu_{\text{CHSH}}(0, 2) = \frac{1}{2}$ and $\mu_{\text{CHSH}}(x, y) = 0$ otherwise. This game is equivalent to choosing to play either the CHSH game or the game corresponding to checking the alignment of the inputs $(0, 2)$ uniformly at random and then proceeding with the chosen game. The frequency distribution then tells us the relative frequencies with which we win each game. The motivation behind $\mathcal{G}_{\text{CHSH}}$ can be understood by considering a schematic of an ideal implementation on a bipartite qubit system as given in Fig. 1. If we observe the maximum winning probability for the CHSH game, as well as perfect alignment for the inputs $(0, 2)$, then the inputs $(\tilde{x}, \tilde{y}) = (1, 2)$ should produce two perfectly uniform bits.

2.4 Device-independent randomness expansion protocols and their security

A device-independent randomness expansion protocol is a procedure by which one attempts to use a uniform, trusted seed, $\mathbf{D}$, to produce a longer uniform bit-string, $\mathbf{Z}$, through repeated interactions with some untrusted devices. We consider so-called *spot-checking* protocols, which involve two round types: test-rounds, during which one attempts to produce certificates of nonlocality, and generation rounds in which a fixed input is given to the devices and the outputs are recorded. By choosing the rounds randomly according to a distribution heavily favouring generation rounds, we are able to reduce the size of the seed whilst sufficiently constraining the device's behaviour, guaranteeing the presence of randomness in the outcomes (except with some small probability).

Using the setup described in Sec. 2.3, our template randomness expansion protocol consists of two main steps.

1. **Accumulation**: In this phase the user repeatedly interacts with the separated devices. Each interaction is randomly chosen to be a generation round or a test round in a coordinated way using the initial

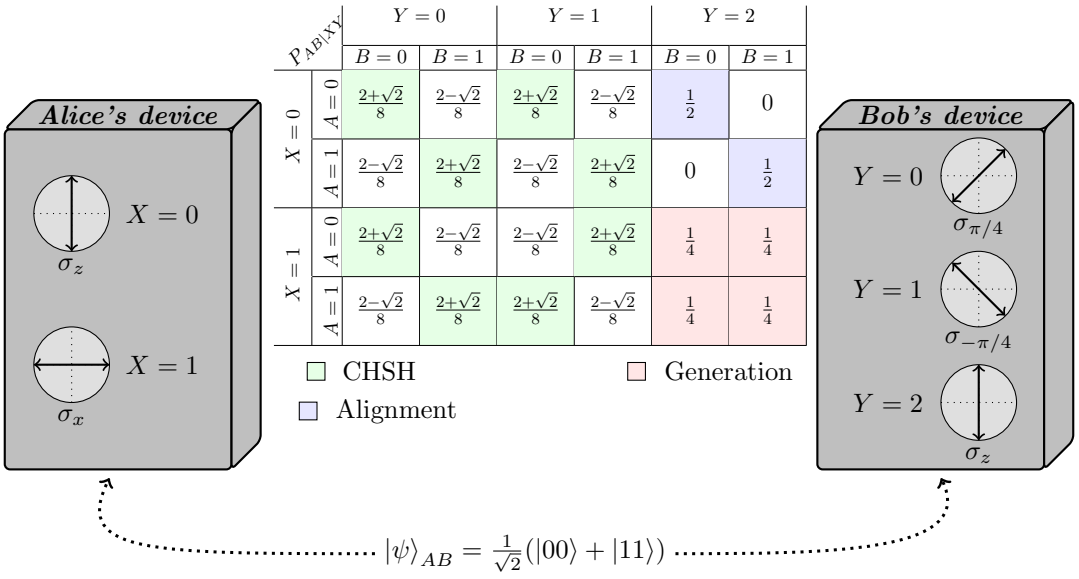


Figure 1: A measurement schematic for a qubit implementation of $\mathcal{G}_{\text{CHSH}}$. Measurements are depicted in the x-z plane of the Bloch-sphere with $\sigma_\varphi = \cos(\varphi)\sigma_z + \sin(\varphi)\sigma_x$ for $\varphi \in (-\pi, \pi]$. Using the maximally entangled state $|\psi\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$ with the measurements depicted, one has a frequency distribution of $\boldsymbol{\omega}_{\mathcal{G}} = \frac{1}{2}\left(\frac{1}{2} + \frac{\sqrt{2}}{4}, 1, \frac{1}{2} - \frac{\sqrt{2}}{4}\right)$, where the scores are ordered $(c_{\text{CHSH}}, c_{\text{align}}, 0)$. The setup achieves Tsirelson's bound for the CHSH game as well as perfect correlations for the $X = 0$ and $Y = 2$ inputs. In addition, self-testing results [38] give a converse result: these scores completely characterize the devices up to local isometries. This implies that the state used by the devices is uncorrelated with an adversary and that the measurement pair $(X, Y) = (1, 2)$ yields uniformly random results, certifying the presence of 2 bits of private randomness in the outputs.

random seed.[9] On generation rounds the devices are provided with some fixed inputs $(\tilde{x}, \tilde{y}) \in \mathcal{X}\mathcal{Y}$, whereas during test rounds, the testing procedure specific to the protocol is followed. After many interactions, the recorded outputs are concatenated to give **AB**. Using the statistics collected during test rounds, a decision is made about whether to abort or not based on how close the observations are to some pre-defined expected device behaviour.

2. **Extraction**: Subject to the protocol not aborting in the accumulation step, a quantum-proof randomness extractor is applied to **AB**. This maps the partially random **AB** to a shorter string **Z** that is the output of the protocol.

We define security of a randomness expansion protocol according to a composable definition [39–43]. Using composable security ensures that the output randomness can be used in any other application with only an arbitrarily small probability of it being distinguishable from perfect randomness. To make this more precise, consider a hypothetical device that outputs a string **Z** that is uniform and uncorrelated with any information held by an eavesdropper. In other words, it outputs $\tau_m \otimes \rho_E$, where τ_m is the maximally mixed state on m qubits. The ideal protocol is defined as the protocol that involves first doing the real protocol, then, in the case of no abort, replacing the output with a string of the same length taken from the hypothetical device. The protocol is then said to be $\varepsilon_{\text{sound}}$-secure ($\varepsilon_{\text{sound}}$ is called the *soundness error*) if, when the user either implements the real or ideal protocol with probability $\frac{1}{2}$, the maximum probability that a distinguisher can guess which is being implemented is at most $\frac{1+\varepsilon_{\text{sound}}}{2}$. If $\varepsilon_{\text{sound}}$ is small, then the real and ideal protocols are virtually indistinguishable. Defining the ideal as above ensures that the real and ideal protocols can never

[9] For example, a central source of randomness could be used to choose the round type. This information could then be communicated to each party (in such a way that the devices do not learn this choice).

be distinguished by whether or not they abort. We refer to [43] for further discussion of composability in a related context (that of QKD).

There is a second important parameter of any protocol, its *completeness error*, which is the probability that an ideal implementation of the protocol leads to an abort. It is important for a protocol to have a low completeness error in addition to a low soundness error since a protocol that always aborts is vacuously secure.

Definition 2.2: Consider a randomness expansion protocol whose output is denoted by Z. Let Ω be the event that the protocol does not abort. The protocol is an $(\varepsilon_{\text{sound}}, \varepsilon_{\text{comp}})$-randomness expansion protocol if it satisfies the following two conditions.

1. **Soundness**:
$$\frac{1}{2}\Pr[\Omega] \cdot \|\rho_{ZE} - \tau_m \otimes \rho_E\|_1 \leq \varepsilon_{\text{sound}}, \tag{13}$$
where E is an arbitrary quantum register (which could have been entangled with the devices used at the start of the protocol), m is the length of the output string Z and τ_m is the maximally mixed state on a system of dimension 2^m.

2. **Completeness**: There exists a set of quantum states and measurements such that if the protocol is implemented using those
$$\Pr[\Omega] \geq 1 - \varepsilon_{\text{comp}}. \tag{14}$$

Although we use a composable security definition to ensure that any randomness output by the protocol can be used in any scenario, importantly, this may not apply if the devices used in the protocol are subsequently reused [44]. Thus, after the protocol the devices should be kept shielded and not reused until such time as the randomness generated no longer needs to be kept secure. How best to resolve this remains an open problem: the Supplemental Material of [44] presents candidate protocol modifications (and modifications to the notion of composability) that may circumvent such problems.

2.5 Entropy accumulation

In order to bound the smooth min entropy $H_{\min}^{\epsilon}(\mathbf{AB}|\mathbf{XY}E)$ accumulated during the protocol we employ the EAT [13, 23]. Roughly speaking, the EAT says that this min-entropy is proportional to the number of rounds, up to square root correction factors. The proportionality constant is the single-round conditional von Neumann entropy optimized over all states that can give rise to the observed scores. In its full form, the EAT is an extension of the asymptotic equipartition property [45] to a particular non-i.i.d. regime. For the purposes of randomness expansion we only require a special case of the EAT, which we detail later in this section.

With the goal of maximising our entropic yield, we use the recently improved statement of the entropy accumulation theorem [23].[10] For completeness we present the relevant statements including the accumulation procedure (see also [15]).

2.5.1 The entropy accumulation procedure

The entropy accumulation procedure prescribes how the user interacts with their untrusted devices and collects data from them. Before beginning this procedure a nonlocal game $\mathcal{G} = (\mu, V)$ that is compatible with the alphabets of the devices is selected.

A *round* within the entropy accumulation procedure consists of the user giving an input to each of their devices and recording the outputs. We use subscripts on random variables to indicate the round that they are associated with, i.e., X_iY_i are the random variables describing the joint device inputs for the i^{th} round. In addition, boldface will be used to indicate that a random variable represents the concatenation over all n rounds of the protocol, $\mathbf{X} = X_1X_2 \ldots X_n$.

The accumulation procedure consists of $n \in \mathbb{N}$ separate interactions with the untrusted devices. We refer to a single interaction with the devices as a *round*. A round consists of the user selecting and supplying inputs to the devices, receiving outputs and recording this data. During the i^{th} round, a random variable

[10] We discuss this EAT statement and compare it to alternatives in Appendix C.

$T_i \sim \text{Bernoulli}(\gamma)$ is sampled, for some fixed $\gamma \in (0,1)$, indicating whether the round will be a *generation round* or a *test round*. With probability $1-\gamma$ we have $T_i = 0$ and the round is a generation round. During a generation round, the user supplies the respective devices with the fixed generation inputs $(\tilde{x}, \tilde{y}) \in \mathcal{X}\mathcal{Y}$, recording $X_i Y_i = (\tilde{x}, \tilde{y})$. They record the outputs received from the devices as A_i and B_i respectively and they record the round's score as $C_i = \perp$. With probability γ, $T_i = 1$ and the round is a test round. During a test round, inputs $X_i Y_i$ are sampled according to the distribution specified by the chosen nonlocal game. The sampled inputs are fed to their respective devices and the outputs received are recorded as $A_i B_i$. The score is computed and recorded as $C_i = V(A_i, B_i, X_i, Y_i)$. The *transcript for round* i is the tuple $(A_i, B_i, X_i, Y_i, T_i, C_i)$. After n rounds, the complete transcript for the accumulation procedure is $(\mathbf{A}, \mathbf{B}, \mathbf{X}, \mathbf{Y}, \mathbf{T}, \mathbf{C})$. We denote by $\mathcal{C}$ the set of possible values that C_i can take, i.e. $\mathcal{C} = \mathcal{G} \cup \{\perp\}$.

After the n-round transcript has been obtained, the user looks to determine the performance of the untrusted devices and, in turn, certify a lower bound on the total entropy produced, $H_{\min}^{\epsilon}(\mathbf{AB}|\mathbf{XY}\text{E})$. To this end, the user computes the *empirical frequency distribution*

$$F_{\mathbf{C}}(c) = \frac{1}{n} \sum_{i=1}^{n} \delta_{c, C_i}. \tag{15}$$

Prior to the accumulation step, the user fixes some frequency distribution $\boldsymbol{\omega}$ corresponding to an expected (or hoped for) behaviour. Should the devices behave in an i.i.d. manner according to $\boldsymbol{\omega}$, then concentration bounds tell us that the empirical frequency distribution $\boldsymbol{F}_{\mathbf{C}}$ should be close to $\boldsymbol{\omega}$. With this in mind, we define the event that the protocol does not abort by

$$\Omega = \{\mathbf{C} \mid \gamma(\boldsymbol{\omega}(\mathcal{G}) - \boldsymbol{\delta}) < \boldsymbol{F}_{\mathbf{C}}(\mathcal{G}) < \gamma(\boldsymbol{\omega}(\mathcal{G}) + \boldsymbol{\delta})\}, \tag{16}$$

where $\boldsymbol{\delta} \in (0,1)^{|\mathcal{G}|}$ is a vector of confidence interval widths satisfying $\mathbf{0} < \boldsymbol{\delta} < \boldsymbol{\omega}(\mathcal{G})$ with all vector inequalities being interpreted as element-wise constraints.

2.5.2 The entropy accumulation theorem

To complete the protocol, uniform randomness needs to be extracted from the partially random outputs. Doing so requires the user to assume a lower bound on the smooth min-entropy (conditioned on any side information held by an adversary) contained in the devices' outputs when the protocol does not abort. If $\varepsilon_{\text{sound}}$ is very small, then the assumption must be correct with near certainty. The EAT provides a method by which one can compute such a lower bound. Loosely, the EAT states that if the interaction between the honest parties occurs in a sequential manner (as described in Sec. 2.5.1), then with high probability the uncertainty an adversary has about the outputs is *close* to their total average uncertainty. As a mathematical statement it is a particular example of the more general phenomenon of *concentration of measure* (see [46] for a general overview). In order to state the EAT precisely, we first require a few definitions.

Definition 2.3 (EAT channels)**:** A set of *EAT channels* $\{\mathcal{N}_i\}_{i=1}^{n}$ is a collection of trace-preserving and completely-positive maps $\mathcal{N}_i : \mathcal{S}(R_{i-1}) \to \mathcal{S}(A_i B_i X_i Y_i C_i R_i)$ such that for every $i \in [n]$:

1. A_i, B_i, X_i, Y_i and C_i are finite dimensional classical systems, R_i is an arbitrary quantum system and C_i is the output of a deterministic function of the classical registers A_i, B_i, X_i and Y_i.

2. For any initial state $\rho_{R_0 E}$, the final state $\rho_{\mathbf{ABXYC}E} = \text{Tr}_{R_n}\left[(\mathcal{N}_n \circ \cdots \circ \mathcal{N}_1) \otimes \mathcal{I}_E)\rho_{R_0 E}\right]$ fulfils the Markov chain condition $I(A^{i-1}B^{i-1}{:}X_i Y_i | X^{i-1}Y^{i-1}E) = 0$ for every $i \in [n]$.

The EAT channels formalise the notion of interaction within the protocol. The first condition in Def. 2.3 specifies the nature of the information present within the protocol and, in particular, it restricts the honest parties' inputs to their devices to be classical in nature. The arbitrary quantum register R_i represents the quantum state stored by the separate devices after the i^{th} round. The second condition specifies the sequential nature of the protocol. The channels $\mathcal{N}_i$ describe the joint action of both devices and include the generation of the randomness needed to choose the settings. The Markov chain condition implies that the inputs to the devices presented by the honest parties are conditionally independent of the previous outputs they have received. Note that by using a trusted private seed to choose the inputs and supplying the inputs

sequentially (as is done in Sec. 2.5.1), this condition will be satisfied.[11] Finally, the adversary is permitted to hold a purification, E of the initial state shared by the devices, and the state evolves with the sequential interaction through the application of the sequence of EAT channels.

As explained above, the EAT allows the elevation of i.i.d. analyses to the non-i.i.d. setting. To do so requires a so-called *min-tradeoff function* which, roughly speaking, gives a lower bound on the single-round von Neumann entropy produced by any devices that, on expectation, produce some statistics. In the case of the EAT these distributions are $\{F_{\mathbf{C}}\}_{\mathbf{C}\in\Omega}$, i.e., all frequency distributions induced from score transcripts $\mathbf{C}$ that do not lead to an aborted protocol. The EAT asserts that, under sequential interaction, an adversary's uncertainty about the outputs of the non-i.i.d. device will (with high probability) be concentrated within some interval about the uncertainty produced by these i.i.d. devices. In particular, a lower bound on this uncertainty can be found by considering the worst-case i.i.d. device.

Definition 2.4 (Min-tradeoff functions)**:** Let $\{\mathcal{N}_i\}_{i=1}^n$ be a collection of EAT channels and let $\mathcal{C}$ denote the common alphabet of the systems $C_1,\ldots,C_n$. An affine function $f:\mathcal{P}_{\mathcal{C}}\to\mathbb{R}$ is a *min-tradeoff function* for the EAT channels $\{\mathcal{N}_i\}_{i=1}^n$ if for each $i\in[n]$ it satisfies

$$f(\boldsymbol{p}) \leq \inf_{\sigma_{R_{i-1}R'}:\mathcal{N}_i(\sigma)_{C_i}=\tau_{\boldsymbol{p}}} H(A_iB_i|X_iY_iR')_{\mathcal{N}_i(\sigma)}, \tag{17}$$

where $\tau_{\boldsymbol{p}} := \sum_{c\in\mathcal{C}} p(c)\,|c\rangle\langle c|$, R' is a register isomorphic to R_{i-1} and the infimum over the empty set is taken to be $+\infty$.

Remark 2.2: As the probability of testing during the protocol is fixed, the expected frequency distributions will always take the form

$$\boldsymbol{p} = \begin{pmatrix} \gamma\boldsymbol{\omega} \\ (1-\gamma) \end{pmatrix} \tag{18}$$

for some $\boldsymbol{\omega}\in\mathcal{Q}_{\mathcal{G}}$, where $p(\perp)$ is the final element of $\boldsymbol{p}$. Furthermore, the fixed testing probability means that any distribution that results in a finite infimum in (17) necessarily takes this form. We shall refer to a distribution of the form (18) as a *protocol-respecting* distribution, denoting the set of all such distributions by Γ.

Particular properties of the min-tradeoff function that appear within the error terms of the EAT are:

- The maximum value attainable on $\mathcal{P}_{\mathcal{C}}$,

$$\mathrm{Max}[f] := \max_{\boldsymbol{p}\in\mathcal{P}_{\mathcal{C}}} f(\boldsymbol{p}). \tag{19}$$

- The minimum value over protocol-respecting distributions,

$$\mathrm{Min}[f|_{\Gamma}] := \min_{\boldsymbol{p}\in\Gamma} f(\boldsymbol{p}). \tag{20}$$

- The maximum variance over all protocol-respecting distributions,

$$\mathrm{Var}[f|_{\Gamma}] := \max_{\boldsymbol{p}\in\Gamma} \sum_{c\in\mathcal{C}} p(c)\left(f(\mathbf{e}_c) - f(\boldsymbol{p})\right)^2. \tag{21}$$

Theorem 2.1 (EAT [23])**:**
Let $\{\mathcal{N}_i\}_{i=1}^n$ be a collection of EAT channels and let $\rho_{\mathbf{ABIC}E} = \mathrm{Tr}_{R_n}\left[(\mathcal{N}_n\circ\cdots\circ\mathcal{N}_1)\otimes\mathcal{I}_E)\rho_{R_0E}\right]$ be the output state after the sequential application of the channels $\{\mathcal{N}_i\otimes\mathcal{I}_E\}_i$ to some input state ρ_{R_0E}. Let $\Omega\subseteq\mathcal{C}^n$ be some event that occurs with probability p_Ω and let $\rho_{|\Omega}$ be the state conditioned on Ω occurring. Finally let

[11] A public seed can also be used if the Markov chain conditions can be shown to hold. However, one may need to be more careful when dealing with such a scenario. For example, if the entangled states distributed to the devices come from some third-party source, then it should be clear that the state used within the i^{th} round was prepared independently of the seed used to generate the inputs $X_{i+1}^nY_{i+1}^n$. This could be achieved by choosing inputs $X_{i+1}Y_{i+1}$ using a public seed that was generated after the i^{th} entangled state has been distributed.

$\epsilon_s \in (0,1)$ *and* f *be a valid min-tradeoff function for* $\{\mathcal{N}_i\}_i$*. If for all* $\mathbf{C} \in \Omega$*, with* $\Pr[\mathbf{C}] > 0$*, there is some* $t \in \mathbb{R}$ *for which* $f(\boldsymbol{F}_{\mathbf{C}}) \geq t$*, then for any* $\beta \in (0,1)$

$$H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathbf{XY}\mathrm{E})_{\rho_{|\Omega}} > nt - n(\epsilon_V + \epsilon_K) - \epsilon_\Omega, \tag{22}$$

where

$$\epsilon_V := \frac{\beta \ln 2}{2}\left(\log\left(2|\mathcal{AB}|^2 + 1\right) + \sqrt{\mathrm{Var}[f|_\Gamma] + 2}\right)^2, \tag{23}$$

$$\epsilon_K := \frac{\beta^2}{6(1-\beta)^3 \ln 2}\, 2^{\beta(\log|\mathcal{AB}| + \mathrm{Max}[f] - \mathrm{Min}[f|_\Gamma])} \ln^3\left(2^{\log|\mathcal{AB}| + \mathrm{Max}[f] - \mathrm{Min}[f|_\Gamma]} + \mathrm{e}^2\right) \tag{24}$$

and

$$\epsilon_\Omega := \frac{1}{\beta}\left(1 - 2\log(p_\Omega\, \epsilon_s)\right). \tag{25}$$

Remark 2.3: As the EAT holds for all $\beta \in (0,1)$ we can numerically optimize our choice of β once we know the values of the other protocol parameters. However, for large n and small γ, a short calculation shows that choosing $\beta \in O(\sqrt{\gamma/n})$ keeps all the error terms of approximately the same magnitude. In particular, this choice results in the error scalings: $n\epsilon_V \in O(\sqrt{n/\gamma})$, $n\epsilon_K \in O(1)$ and $\epsilon_\Omega \in O(\sqrt{n/\gamma})$.

2.6 Randomness extractors

Subject to the protocol not aborting, the entropy accumulation sub-procedure detailed in Sec. 2.5.1 will result in the production of some bit string $\mathbf{AB} \in \{0,1\}^{2n}$ with $H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathbf{XY}\mathrm{E}) > k$ for some $k \in \mathbb{R}$. In order to 'compress' this randomness into a shorter but almost uniform random string a *seeded, quantum-proof randomness extractor* can be used. This is a function $R_{\mathrm{ext}} : \mathbf{AB} \times \mathbf{D} \to \mathbf{Z}$, such that if $\mathbf{D}$ is a uniformly distributed bit-string, the resultant bit-string $\mathbf{Z}$ is ϵ-close to uniformly distributed, even from the perspective an adversary with quantum side-information E about $\mathbf{AB}$. More formally, combining [47, Lemma 3.5] with the standard definition for a quantum-proof randomness extractor [48] gives the following definition.

Definition 2.5 (Quantum-proof strong extractor)**:** A function $R_{\mathrm{ext}} : \{0,1\}^{|\mathbf{AB}|} \times \{0,1\}^{|\mathbf{D}|} \to \{0,1\}^{|\mathbf{Z}|}$ is a *quantum-proof* $(k, \epsilon_{\mathrm{ext}} + 2\epsilon_s)$*-strong extractor*, if for all cq-states $\rho_{\mathbf{AB}\mathrm{E}}$ with $H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathrm{E})_\rho \geq k$ and for some $\epsilon_s > 0$ it maps $\rho_{\mathbf{AB}\mathrm{E}} \otimes \tau_{\mathbf{D}}$ to $\rho'_{R_{\mathrm{ext}}(\mathbf{AB},\mathbf{D})\mathbf{D}\mathrm{E}}$ where

$$\frac{1}{2}\|\rho'_{R_{\mathrm{ext}}(\mathbf{AB},\mathbf{D})\mathbf{D}\mathrm{E}} - \tau_m \otimes \tau_{|\mathbf{D}|} \otimes \rho_{\mathrm{E}}\|_1 \leq \epsilon_{\mathrm{ext}} + 2\epsilon_s\,. \tag{26}$$

(Recall that τ_m is the maximally mixed state on a system of dimension m.)

Although in general the amount of randomness extracted will depend on the extractor, $H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathrm{E})$ provides an upper bound on the total number of ϵ_s-close to uniform bits that can be extracted from $\mathbf{AB}$ and a well-chosen extractor will result in a final output bit-string with $|\mathbf{Z}| \approx H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathrm{E})$. We denote any loss of entropy incurred by the extractor by $\ell_{\mathrm{ext}} = k - |\mathbf{Z}|$. Entropy loss will differ between extractors but in general it will be some function of the extractor error, the seed length and the initial quantity of entropy. The extractor literature is rich with explicit constructions, with many following Trevisan's framework [49]. For an in-depth overview of randomness extraction, we refer the reader to [50] and references therein.

Remark 2.4: By using a *strong* quantum-proof extractor, the output of the extractor will remain uncorrelated with the string used to seed it. Since the seed acts like a catalyst, we need not be overly concerned with the amount required. Furthermore, if available, it could just be acquired from a trusted public source immediately prior to extraction without compromising security. However, if a public source is used, it is important that it is not available to Eve too early in the protocol as this could allow Eve to create correlations between the outputs of the devices and the extractor seed.

Remark 2.5: Related to the previous remark is the question of whether the quantity we are interested in is $H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathbf{XY}\mathrm{E})$, rather than $H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathrm{E})$ or $H_{\min}^{\epsilon_s}(\mathbf{ABXY}|\mathrm{E})$. In common QKD protocols (such as BB84), the first of these is the only reasonable choice because the information $\mathbf{XY}$ is communicated between the two parties over an insecure channel and hence could become known by Eve. For randomness expansion, this

is no longer the case: this communication can all be kept secure within one lab. Whether the alternative quantities can be used then depends on where the seed randomness comes from. If a trusted beacon is used then the first case is needed. If the seed randomness can be kept secure until such time that the random numbers need no longer be kept random then the second quantity could be used[12]. If it is also desirable to extract as much randomness as possible, then the third quantity could be used instead. However, in many protocols the amount of seed required to choose X and Y in the entropy accumulation procedure is small enough that extracting randomness from this will not significantly increase the rate (see, e.g., our discussion in Appendix B).

3 A template protocol for randomness expansion

The primary purpose of this work is to provide a method whereby one can construct tailored randomness expansion protocols, with a guarantee of security and easily calculable generation rates. We achieve this by providing a template protocol (Protocol QRE), for which we have explicit security statements in terms of the protocol parameters as well as the outputs of some SDPs. Our framework is divided into three sub-procedures: preparation, accumulation and extraction.

The preparation procedure consists of assigning values to the various parameters of the protocol, this includes choosing a nonlocal game to act as the nonlocality test. At the end of the preparation one would have turned the protocol template into a precise protocol, constructed a min-tradeoff function and be able to calculate the relevant security quantities. Note that once a specific protocol has been decided it is not necessary to perform this step. Furthermore, the manufacturer may already specify the entire protocol to use with their devices, in which case this step can be skipped. Nevertheless, the fact that the protocol can be tuned to the devices at hand enables the user to optimize the randomness output from the devices at hand.

The final two parts of the framework form the process described in Protocol QRE. The accumulation step follows the entropy accumulation procedure detailed in Sec. 2.5.1 wherein the user interacts with their devices using the chosen protocol parameters. After the device interaction phase has finished, the user implicitly evaluates the quality of their devices by testing whether the observed inputs and outputs satisfy the condition (16). Subject to the protocol not aborting, a reliable lower bound on the min-entropy of the total output string is calculated through the EAT (22). With this bound, the protocol can be completed by applying an appropriate quantum-proof randomness extractor to the devices' raw output strings.

The next three subsections are dedicated to explaining these three sub-procedures in detail. In particular, Sec. 3.1 outlines the min-tradeoff function construction. A bound on the total entropy accumulated in terms of the various protocol parameters is then provided in Sec. 3.2 and finally, in Sec. 3.3, the security statements for the template protocol are presented.

3.1 Preparation

Before interacting with their devices the user must select appropriate protocol parameters (see Fig. 2 for a full list of parameters). In particular, they must choose a nonlocal game to use during the test rounds and construct a corresponding min-tradeoff function. This step enables this to be done if it is not already specified.

The parameter values chosen will largely be dictated by situational constraints; e.g., runtime, seed length and the expected performance of the untrusted devices.[13] The user's choice of parameters, in particular the choice of nonlocal game, will affect the form of their min-tradeoff function derived and in turn their projected total accumulated entropy. Before moving to the accumulation step of the protocol the user can try to optimise their chosen parameters by computing the entropy rates for many different choices. This allows them to adapt their protocol to the projected performance of their devices.

[12] This is a reasonable requirement, because there are other strings that have to be kept secure in the same way, e.g., the raw string $\mathbf{A}$.

[13] At first this may seem to conflict with the ethos of device-independence. The point is that although the user of the protocol relies on an expected behaviour to set-up their devices, they do not rely on this expected behaviour being an accurate reflection of the devices for security. This also means that the expected behaviour could be that claimed by the device manufacturer. Using inaccurate estimation of the devices behaviour will not compromise security, but may lead to a different abort probability.

Protocol QRE

Parameters and notation:

$\mathfrak{D}_{AB}$ – a pair of untrusted devices taking inputs from $\mathcal{X}$, $\mathcal{Y}$ and giving outputs from $\mathcal{A}$, $\mathcal{B}$

$\mathcal{G} = (\mu, V)$ – a nonlocal game compatible with $\mathfrak{D}_{AB}$

$\boldsymbol{\omega} \in \mathcal{Q}_{\mathcal{G}}$ – an expected frequency distribution for $\mathcal{G}$

$\boldsymbol{\delta}$ – vector of confidence interval widths (satisfies $0 \leq \delta_k \leq \omega_k$ for all $k \in [|\mathcal{G}|]$)

$n \in \mathbb{N}$ – number of rounds

$\gamma \in (0, 1)$ – probability of a test round

$(\tilde{x}, \tilde{y})$ – distinguished inputs for generation rounds

$f_{\min}$ – min-tradeoff function

$\epsilon_{\text{ext}} > 0$ – extractor error

$\epsilon_s \in (0, 1)$ – smoothing parameter

$\epsilon_{\text{EAT}} \in (0, 1)$ – entropy accumulation error

R_{ext} – quantum-proof $(k, \epsilon_{\text{ext}} + 2\epsilon_s)$-strong extractor

ℓ_{ext} – entropy loss induced by R_{ext}

Procedure:

1: Set $i = 1$.

2: **While** $i \leq n$:

Choose $T_i = 0$ with probability $1 - \gamma$ and otherwise $T_1 = 1$.

If $T_i = 0$:

Gen: Input $(\tilde{x}, \tilde{y})$ into the respective devices, recording the inputs $X_i Y_i$ and outputs $A_i B_i$. Set $C_i = \perp$ and $i = i + 1$.

Else:

Test: Play a single round of $\mathcal{G}$ on $\mathfrak{D}_{AB}$ using inputs sampled from μ, recording the inputs $X_i Y_i$ and outputs $A_i B_i$. Set $C_i = V(A_i, B_i, X_i, Y_i)$ and $i = i + 1$.

3: Compute the empirical frequency distribution $\boldsymbol{F}_{\mathbf{C}}$.

If $\gamma(\boldsymbol{\omega} - \boldsymbol{\delta}) < \boldsymbol{F}_{\mathbf{C}}(\mathcal{G}) < \gamma(\boldsymbol{\omega} + \boldsymbol{\delta})$:

Ext: Apply a strong quantum-proof randomness extractor R_{ext} to the raw output string $\mathbf{AB}$ producing $n f_{\min}(\boldsymbol{\omega} - \boldsymbol{\delta}_{\text{sgn}}) - \ell_{\text{ext}}$ bits $(\epsilon_{\text{ext}} + 2\epsilon_s)$-close to uniformly distributed.

Else:

Abort: Abort the protocol.

Figure 2: The template quantum-secure device-independent randomness expansion protocol.

We now present a constructible family of min-tradeoff functions for a general instance of Protocol QRE. This construction is based on the following idea. As noted in Sec. 2.2 one can numerically calculate a lower bound on the min-entropy of a system based on its observed statistics. Pairing this with the relation, $H_{\min}(X|E) \leq H(X|E)$, we have access to numerical bounds on the von Neumann entropy. In particular, we can use the affine function $g(\boldsymbol{q}) = \boldsymbol{\lambda} \cdot \boldsymbol{q}$, where $\boldsymbol{\lambda}$ is a feasible point of the dual program (10), in order to build a min-tradeoff function for the protocol.[14] In order for g to meet the requirements of a min-tradeoff function, its domain must be extended to include the symbol $\perp$. To perform this extension we use the method presented in [23, Section 5.1]. As the rounds are split into testing and generation rounds, we may decompose the EAT-channel for the i^{th} round as $\mathcal{N}_i = \gamma \mathcal{N}_i^{\text{test}} + (1 - \gamma)\mathcal{N}_i^{\text{gen}}$, where $\mathcal{N}_i^{\text{test}}$ is the channel that would be applied if the round were a test round and $\mathcal{N}_i^{\text{gen}}$ if the round were a generation round. Importantly, this splitting

[14] In fact, by relaxing the dual program to the NPA hierarchy, the single round bound is valid against super-quantum adversaries. However, the full protocol is not necessarily secure more widely: to show that we would need to generalise the EAT and the extractor.

separates $\perp$ from the nonlocal game scores. That is, if $\mathcal{N}_i^{\text{test}}$ is the channel applied then $\Pr[C_i = \perp] = 0$ whereas if $\mathcal{N}_i^{\text{gen}}$ is applied then $\Pr[C_i = \perp] = 1$.

Lemma 3.1 (Min-tradeoff extension [23, Lemma 5.5])**:** *Let $g : \mathcal{P}_{\mathcal{G}} \to \mathbb{R}$ be an affine function satisfying*

$$g(\boldsymbol{p}) \leq \inf_{\sigma_{R_{i-1}R'} : \mathcal{N}_i^{\text{test}}(\sigma)_{C_i} = \tau_{\boldsymbol{p}}} H(A_iB_i|X_iY_iR')_{\mathcal{N}_i(\sigma)} \tag{27}$$

for all $\boldsymbol{p} \in \mathcal{Q}_{\mathcal{G}}$. Then, the function $f : \mathcal{P}_{\mathcal{G}\cup\{\perp\}} \to \mathbb{R}$, defined by its action on trivial distributions

$$\begin{aligned} f(\mathbf{e}_c) &= \text{Max}[g] + \frac{g(\mathbf{e}_c) - \text{Max}[g]}{\gamma}, \qquad \forall c \in \mathcal{G}, \\ f(\mathbf{e}_\perp) &= \text{Max}[g], \end{aligned}$$

is a min-tradeoff function for the EAT-channels $\{\mathcal{N}_i\}_i$. Furthermore, f satisfies the following properties:

$$\begin{aligned} \text{Max}[f] &= \text{Max}[g], \\ \text{Min}[f|_\Gamma] &\geq \text{Min}[g], \\ \text{Var}[f|_\Gamma] &\leq \frac{(\text{Max}[g] - \text{Min}[g])^2}{\gamma}. \end{aligned}$$

Lemma 3.2 (Min-tradeoff construction)**:** *Let $\mathcal{G}$ be a nonlocal game and $k \in \mathbb{N}$. For each $\boldsymbol{\nu} \in \mathcal{Q}_{\mathcal{G}}^{(k)}$, let $\boldsymbol{\lambda}_{\boldsymbol{\nu}}$ be a feasible point of Prog.* (10) *when parameterized by $\boldsymbol{\nu}$. Furthermore, let $\lambda_{\max} = \max_{c\in\mathcal{G}} \lambda_{\boldsymbol{\nu}}(c)$ and $\lambda_{\min} = \min_{c\in\mathcal{G}} \lambda_{\boldsymbol{\nu}}(c)$. Then, for any set of EAT channels $\{\mathcal{N}_i\}_{i=1}^n$ implementing an instance of Protocol QRE with the nonlocal game $\mathcal{G}$, the set of functionals $\mathcal{F}_{\min}(\mathcal{G}) = \{f_{\boldsymbol{\nu}}(\cdot) \mid \boldsymbol{\nu} \in \mathcal{Q}_{\mathcal{G}}^{(k)}\}$ forms a family of min-tradeoff functions, where $f_{\boldsymbol{\nu}} : \mathcal{P}_{\mathcal{C}} \to \mathbb{R}$ are defined by their actions on trivial distributions*

$$f_{\boldsymbol{\nu}}(\mathbf{e}_c) := (1-\gamma)\left(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}} \frac{\boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot \mathbf{e}_c - (1-\gamma)\lambda_{\min}}{\gamma}\right) \quad \text{for } c \in \mathcal{G}, \tag{28}$$

and

$$f_{\boldsymbol{\nu}}(\mathbf{e}_\perp) := (1-\gamma)\left(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\, \lambda_{\min}\right), \tag{29}$$

where $A_{\boldsymbol{\nu}} = \frac{1}{\ln 2} - \log(\boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot \boldsymbol{\nu})$ and $B_{\boldsymbol{\nu}} = \frac{1}{\boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot \boldsymbol{\nu} \ln 2}$.

Moreover, these min-tradeoff functions satisfy the following relations.

- *Maximum:*
$$\text{Max}[f_{\boldsymbol{\nu}}] = (1-\gamma)(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\, \lambda_{\min}) \tag{30}$$
- Γ-*Minimum:*
$$\text{Min}[f_{\boldsymbol{\nu}}|_\Gamma] \geq (1-\gamma)(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\, \lambda_{\max}) \tag{31}$$
- Γ-*Variance:*
$$\text{Var}[f_{\boldsymbol{\nu}}|_\Gamma] \leq \frac{(1-\gamma)^2 B_{\boldsymbol{\nu}}^2 (\lambda_{\max} - \lambda_{\min})^2}{\gamma} \tag{32}$$

Proof. Consider the entropy bounding property (27) but with $\mathcal{C}$ restricted to the scoring alphabet of $\mathcal{G}$, i.e., we have an affine function $g_{\boldsymbol{\nu}} : \mathcal{P}_{\mathcal{G}} \to \mathbb{R}$ such that

$$g_{\boldsymbol{\nu}}(\boldsymbol{q}) \leq \inf_{\sigma_{R_{i-1}R'} : \mathcal{N}_i^{\text{test}}(\sigma)_{C_i(\mathcal{G})} = \tau_{\boldsymbol{q}}} H(A_iB_i|X_iY_iR')_{\mathcal{N}_i(\sigma)},$$

for all $\boldsymbol{q} \in \mathcal{Q}_{\mathcal{G}}$.

As conditioning on additional side information will not increase the von Neumann entropy, we may condition on whether or not the round was a test round,

$$\begin{aligned} H(A_iB_i|X_iY_iR')_{\mathcal{N}_i(\sigma)} &\geq H(A_iB_i|X_iY_iT_iR')_{\mathcal{N}_i(\sigma)} \\ &= \gamma H(A_iB_i|X_iY_i, T_i = 1, R')_{\mathcal{N}_i(\sigma)} + (1-\gamma)H(A_iB_i|X_iY_i, T_i = 0, R')_{\mathcal{N}_i(\sigma)} \\ &> (1-\gamma)H(A_iB_i|X_i = \tilde{x}, Y_i = \tilde{y}, T_i = 0, R')_{\mathcal{N}_i(\sigma)} \end{aligned}$$

where in the final line we have used the fact that the inputs are fixed for generation rounds. As the min-entropy lower bounds the von Neumann entropy, we arrive at the bound

$$H(A_iB_i|X_iY_iR')_{\mathcal{N}_i(\sigma)} > (1-\gamma)H_{\min}(A_iB_i|X_i = \tilde{x}, Y_i = \tilde{y}, T_i = 0, R')_{\mathcal{N}_i(\sigma)}.$$

Using programs (9) and (10), we can lower bound the right-hand side in terms of the relaxed guessing probability. Specifically, for a single generation round

$$\begin{aligned} H_{\min}(AB|X = \tilde{x}, Y = \tilde{y}, T = 0, R') &= -\log(p_{\text{guess}}(\boldsymbol{q})) \\ &\geq -\log(\boldsymbol{\lambda}_{\boldsymbol{\nu}}^{(k)} \cdot \boldsymbol{q}), \end{aligned}$$

holds for all $k \in \mathbb{N}$, any $\boldsymbol{\nu} \in \mathcal{Q}_{\mathcal{G}}^{(k)}$ and any quantum system realising the expected statistics $\boldsymbol{q} \in \mathcal{Q}_{\mathcal{G}}$. In the final line we used the monotonicity of the logarithm together with the fact that a solution to the relaxed dual program, for any parameterization $\boldsymbol{\nu} \in \mathcal{Q}_{\mathcal{G}}^{(k)}$, provides a linear function $\boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot (\,\cdot\,)$ that is greater than p_{guess} everywhere on $\mathcal{Q}_{\mathcal{G}}^{(k)}$. Note that this bound is also device-independent and is therefore automatically a bound on the infimum. Dropping the superscript (k) for notational ease, we may recover the desired affine property by taking a first order expansion about the point $\boldsymbol{\nu}$. This results in the function

$$g_{\boldsymbol{\nu}}(\boldsymbol{q}) := (1-\gamma)(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\, \boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot \boldsymbol{q}),$$

which satisfies

$$g_{\boldsymbol{\nu}}(\boldsymbol{q}) \leq \inf_{\sigma_{R_{i-1}R'} : \mathcal{N}_i^{\text{test}}(\sigma)_{C_i} = \tau_{\boldsymbol{q}}} H(A_iB_i|X_iY_iR')_{\mathcal{N}_i(\sigma)},$$

for all $\boldsymbol{q} \in \mathcal{Q}_{\mathcal{G}}$, with $A_{\boldsymbol{\nu}}$ and $B_{\boldsymbol{\nu}}$ as defined in Lemma 3.2. The statement then follows by applying Lemma 3.1 to $g_{\boldsymbol{\nu}}$, noting $\text{Max}[g_{\boldsymbol{\nu}}] = (1-\gamma)(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\, \lambda_{\min})$ and $\text{Min}[g_{\boldsymbol{\nu}}] = (1-\gamma)(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\, \lambda_{\max})$. □

Example 3.1: Taking the nonlocal game $\mathcal{G}_{\text{CHSH}}$ introduced in Example 2.1, we can use the above lemma to construct a min-tradeoff function. Fixing the probability of testing, $\gamma = 5 \times 10^{-3}$, we consider a device that behaves (during a test round) according to the expected frequency distribution $\boldsymbol{\omega} = (\omega_{\text{align}}, \omega_{\text{CHSH}}, 1 - \omega_{\text{align}} - \omega_{\text{CHSH}})$. In Fig. 3, we plot the certifiable min-entropy of a single generation round for a range of $\boldsymbol{\omega}$. We see that as the scores approach $\boldsymbol{\omega} = \frac{1}{2}\left(1, \frac{2+\sqrt{2}}{4}, \frac{2-\sqrt{2}}{4}\right)$, we are able to certify almost[15] two bits of randomness per entangled qubit pair using $\mathcal{G}_{\text{CHSH}}$.

3.2 Accumulation and extraction

After fixing the parameters of the protocol and constructing a min-tradeoff function $f_{\min}$, the user proceeds with the remaining steps of Protocol QRE: accumulation and extraction. The accumulation step consists of the device interaction and evaluation sub-procedures that were detailed in Sec. 2.5.1. If the protocol does not abort, then with high probability the generated string $\mathbf{AB}$ contains at least some given quantity of smooth min-entropy. The following lemma applies the EAT to deduce a lower bound on the amount of entropy accumulated.

Lemma 3.3 (Accumulated entropy)**:** *Let the randomness expansion procedure and all of its parameters be as defined in Fig. 2. Furthermore, let Ω be the event the protocol does not abort (cf.* (16)*) and let $\rho_{|\Omega}$ be the final state of the system conditioned on this. Then, for any β, ϵ_s, $\epsilon_{\text{EAT}} \in (0,1)$ and any choice of min-tradeoff function $f_{\boldsymbol{\nu}} \in \mathcal{F}_{\min}$, either Protocol QRE aborts with probability greater than $1 - \epsilon_{\text{EAT}}$ or*

$$H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathbf{XY}\text{E})_{\rho_{|\Omega}} > (1-\gamma)n\left(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot (\boldsymbol{\omega} - \boldsymbol{\delta}_{\text{sgn}})\right) - n(\epsilon_V + \epsilon_K) - \epsilon_\Omega, \tag{33}$$

[15] Due to the infrequent testing we are actually only able to certify a maximum of $2 \cdot (1-\gamma)$ bits per interaction.

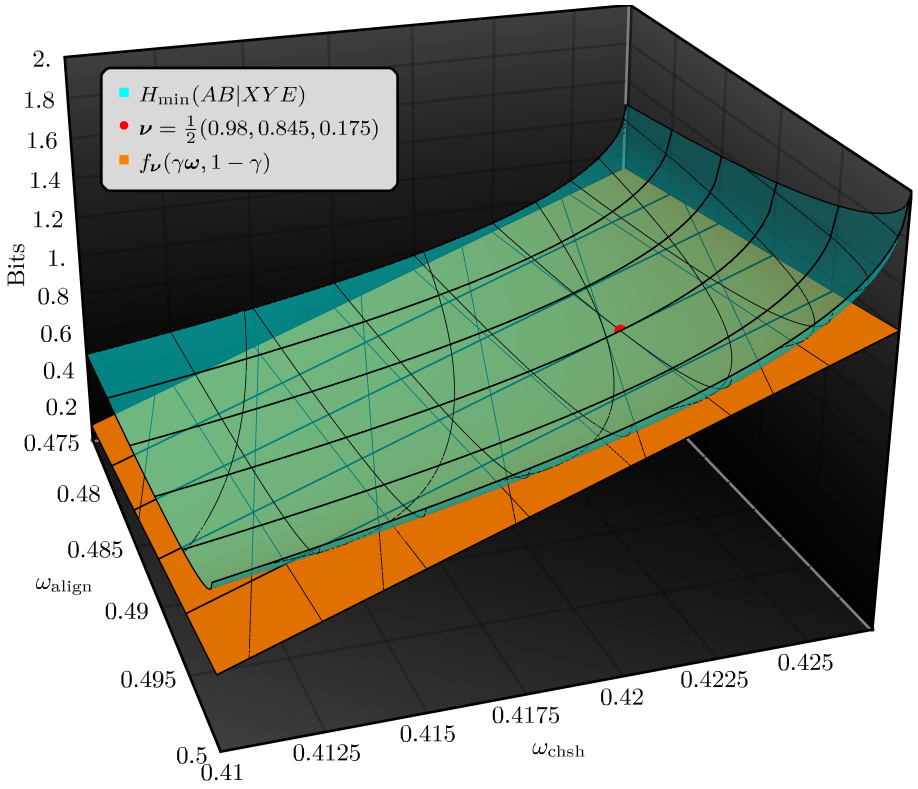


Figure 3: A plot of a lower bound on the certifiable min-entropy produced during a single round of the protocol. This lower bound was calculated using Prog. 9 relaxed to the second level of the NPA hierarchy. In addition, we plot a min-tradeoff function $f_{\boldsymbol{\nu}}$ evaluated for distributions of the form $\boldsymbol{p} = (\gamma\boldsymbol{\omega}, 1-\gamma)$ for $\boldsymbol{\omega} \in \mathcal{Q}_{\mathcal{G}}$, i.e. expected frequency distributions over $\mathcal{G} \cup \{\perp\}$ that are compatible with the spot-checking structure of the rounds. Since $f_{\boldsymbol{\nu}}$ is the tangent plane to the surface at the point $\boldsymbol{\nu}$ it forms an affine lower bound on the min-entropy of any quantum distribution compatible with the protocol.

where

$$\epsilon_V := \frac{\beta \ln 2}{2}\left(\log\left(2|\mathcal{AB}|^2 + 1\right) + \sqrt{\frac{(1-\gamma)^2 B_{\boldsymbol{\nu}}^2 (\lambda_{\max} - \lambda_{\min})^2}{\gamma} + 2}\right)^2, \tag{34}$$

$$\epsilon_K := \frac{\beta^2}{6(1-\beta)^3 \ln 2} 2^{\beta(\log|\mathcal{AB}| + (1-\gamma)B_{\boldsymbol{\nu}}(\lambda_{\max}-\lambda_{\min}))} \ln^3\left(2^{\log|\mathcal{AB}| + (1-\gamma)B_{\boldsymbol{\nu}}(\lambda_{\max}-\lambda_{\min})} + e^2\right), \tag{35}$$

$$\epsilon_\Omega := \frac{1}{\beta}\left(1 - 2\log(\epsilon_{\text{EAT}}\,\epsilon_s)\right) \tag{36}$$

and $\boldsymbol{\delta}_{\text{sgn}} = (\delta(c)\,\text{sgn}(-\lambda_{\boldsymbol{\nu}}(c)))_{c\in\mathcal{G}}$.

Proof. Let $\{\mathcal{N}_i\}_{i\in[n]}$ be the set of channels implementing the entropy accumulation sub-procedure of Protocol QRE. Comparing this procedure with the definition of the EAT channels Def. 2.3, we have $\mathcal{N}_i : \mathcal{S}(R_{i-1}) \to \mathcal{S}(A_iB_iX_iY_iT_iC_iR_i)$ with $A_i, B_i, X_i, Y_i, T_i, C_i$ finite dimensional classical systems, R_i an arbitrary quantum system and the score C_i is a deterministic function of the values of the other classical systems. Furthermore, the inputs to the protocol for the i^{th} round, (X_i, Y_i, T_i), are chosen independently of all other systems in the protocol and so the conditional independence constraints $I(A_1^{i-1}B_1^{i-1}\!:\!X_iY_i|X_1^{i-1}Y_1^{i-1}E) = 0$ hold trivially. The conditions necessary for $\{\mathcal{N}_i\}_{i\in[n]}$ to be EAT-channels are satisfied and by Lemma 3.2 $f_{\boldsymbol{\nu}}$ is a min-tradeoff function for these channels. We can now apply the EAT to bound the total entropy accumulated.

Consider now the pass probability of the protocol, p_Ω. Either $p_\Omega < \epsilon_{\text{EAT}}$, in which case the protocol will abort with probability at least $1 - \epsilon_{\text{EAT}}$, or $p_\Omega \geq \epsilon_{\text{EAT}}$. In the latter case we can replace the unknown p_Ω

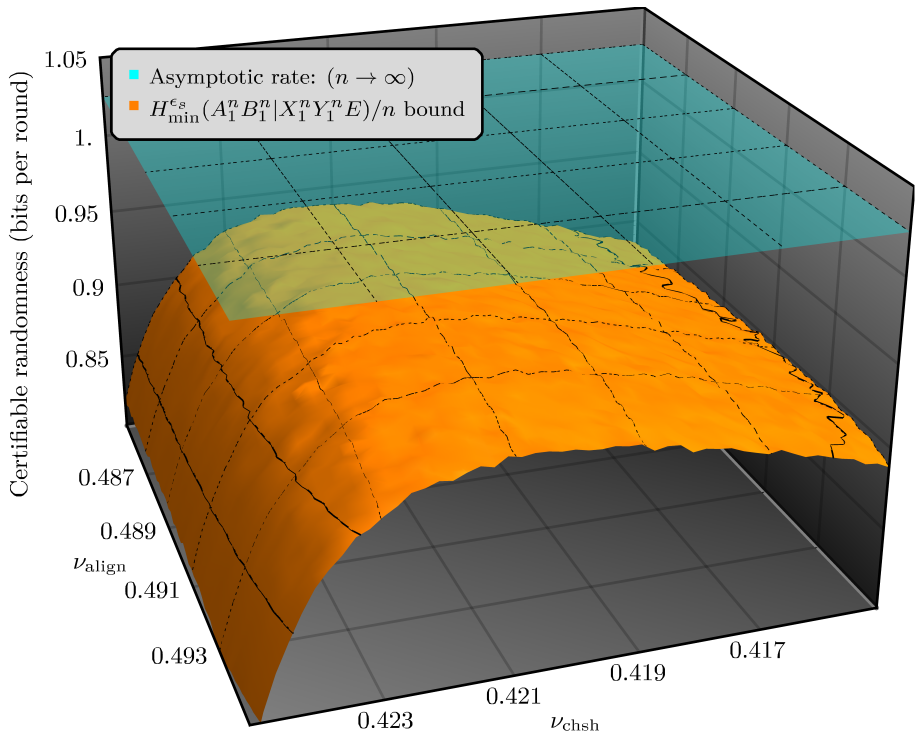


Figure 4: A plot of the randomness certified as we vary our choice of min-tradeoff function. At each point ν we evaluate the certifiable randomness (33) for the corresponding choice of min-tradeoff function f_ν, numerically optimizing the parameter β each time. The rough appearance of the surface is a result of finding local optima in the β optimization. For reference, we include a plot of the asymptotic rate, i.e., (33) as $n \to \infty$ and $\boldsymbol{\delta} \to \mathbf{0}$. The protocol parameters used during the calculations are as follows: $n = 10^{10}$, $\gamma = 5 \times 10^{-3}$, $\boldsymbol{\omega} = (0.49, 0.4225, 0.0875)$, $\delta_{\text{CHSH}} = \delta_{\text{align}} = 10^{-3}$ and $\epsilon_s = \epsilon_{\text{EAT}} = 10^{-8}$.

in (25) with ϵ_{EAT} as this results in an increase in the error term ϵ_Ω. The EAT then asserts that

$$H_{\min}^{\epsilon_s}(\mathbf{AB}|\mathbf{XY}\text{E})_{\rho_{|\Omega}} > n \inf_{\mathbf{C}\in\Omega} f_{\boldsymbol{\nu}}(\boldsymbol{F}_{\mathbf{C}}) - n(\epsilon_V + \epsilon_K) - \epsilon_\Omega,$$

for any choice of min-tradeoff function $f_{\boldsymbol{\nu}} \in \mathcal{F}_{\min}$.

As the min-tradeoff functions are affine, we can lower bound the infimum for the region of possible scores specified by the success event,

$$\Omega = \{\mathbf{C} \mid \gamma(\boldsymbol{\omega} - \boldsymbol{\delta}) < \boldsymbol{F}_{\mathbf{C}}(\mathcal{G}) < \gamma(\boldsymbol{\omega} + \boldsymbol{\delta})\}.$$

Taking $\boldsymbol{p} = (\gamma(\boldsymbol{\omega} - \boldsymbol{\delta}_{\text{sgn}}), (1-\gamma))$, we have $f(\boldsymbol{p}) \leq \inf_{\mathbf{C}\in\Omega} f_{\boldsymbol{\nu}}(\boldsymbol{F}_{\mathbf{C}})$. Note that $\boldsymbol{p}$ may not correspond to a frequency distribution that could have resulted from a successful run of the protocol – it may not even be a probability distribution. However, it is sufficient for our purposes as an explicit lower bound on the infimum. Further, noting that $f_{\boldsymbol{\nu}}(\boldsymbol{p}) = g_{\boldsymbol{\nu}}(\boldsymbol{\omega} - \boldsymbol{\delta}_{\text{sgn}})$, we can straightforwardly compute this lower bound as

$$f_{\boldsymbol{\nu}}(\boldsymbol{p}) = (1-\gamma)\left(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot (\boldsymbol{\omega} - \boldsymbol{\delta}_{\text{sgn}})\right).$$

Inserting the min-tradeoff function properties (30)–(32) into the the EAT's error terms [(23)–(25)] we get the explicit form of the quantities ϵ_V, ϵ_K and ϵ_Ω stated in the lemma. □

If the protocol does not abort during the accumulation procedure, the user may proceed by applying a quantum-proof strong extractor to the concatenated output string $\mathbf{AB}$ resulting in a close to uniform bit-string of length approximately $(1-\gamma)n\left(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot (\boldsymbol{\omega} - \boldsymbol{\delta}_{\text{sgn}})\right) - n(\epsilon_V + \epsilon_K) - \epsilon_\Omega$.

Example 3.2: Continuing from Ex. 3.1, we look at the bound on the accumulated entropy specified by (33) for a range of choices of $f_{\boldsymbol{\nu}} \in \mathcal{F}_{\min}$. Again, we are considering a quantum implementation with an expected frequency distribution $\boldsymbol{\omega} = (0.49, 0.4225, 0.0875)$. In Fig. 4 we see that our choice of min-tradeoff function can have a large impact on the quantity of entropy we are able to certify. The plot gives some reassuring numerical evidence that, for the nonlocal game $\mathcal{G}_{\text{CHSH}}$, the certifiable randomness is continuous and concave in the family parameter $\boldsymbol{\nu}$.

The min-tradeoff function indexed by our expected frequency distribution, $f_{\boldsymbol{\omega}}$, is able to certify just under 0.939-bits per interaction. By applying a gradient-ascent algorithm we were able to improve this to 0.946-bits per interaction. In an attempt to avoid getting stuck within local optima we applied the algorithm several times, starting subsequent iterations at randomly chosen points close to the current optimum. The optimization led to an improved min-tradeoff function choice $f_{\boldsymbol{\nu}^*}$, where $\boldsymbol{\nu}^* = (0.491, 0.421, 0.088)$.

3.3 Protocol QRE

Protocol QRE is the concatenation of the accumulation and extraction sub-procedures. It remains to provide the formal security statements for a general instance of Protocol QRE. We refer to an untrusted device network $\mathfrak{D}_{AB}$ as *honest* if during each interaction, the underlying quantum state shared amongst the devices and the measurements performed in response to inputs remain the same (i.e., the devices behave as the user expects). Furthermore, each interaction is performed independently of all others. The following lemma provides a bound on the probability that an honest implementation of Protocol QRE aborts.

Lemma 3.4 (Completeness of Protocol QRE)**:** *Let Protocol QRE and all of its parameters be as defined in Fig. 2. Then, the probability that an honest implementation of Protocol QRE aborts is no greater than* $\varepsilon_{\text{comp}}$ *where*

$$\varepsilon_{\text{comp}} = 2\sum_{k=1}^{|\mathcal{G}|} \mathrm{e}^{-\frac{\gamma\delta_k^2}{3\omega_k}n}. \tag{37}$$

Proof. During the parameter estimation step of Protocol QRE, the protocol aborts if the observed frequency distribution $\boldsymbol{F}_{\mathbf{C}}$ fails to satisfy

$$\gamma(\boldsymbol{\omega} - \boldsymbol{\delta}) < \boldsymbol{F}_{\mathbf{C}}(\mathcal{G}) < \gamma(\boldsymbol{\omega} + \boldsymbol{\delta}).$$

Writing $\boldsymbol{F}_{\mathbf{C}}(\mathcal{G}) = (r_k)_{k=1}^{|\mathcal{G}|}$, $\boldsymbol{\omega} = (\omega_k)_{k=1}^{|\mathcal{G}|}$ and $\boldsymbol{\delta} = (\delta_k)_{k=1}^{|\mathcal{G}|}$, the probability that an honest implementation of the protocol aborts can be written as

$$\mathrm{P}_{\text{abort}} = \Pr\left[\bigcup_{k=1}^{|\mathcal{G}|}\left\{\left|r_k - \gamma\omega_k\right| \geq \gamma\delta_k\right\}\right] \leq \sum_{k=1}^{|\mathcal{G}|}\Pr\left[\left|r_k - \gamma\omega_k\right| \geq \gamma\delta_k\right].$$

Restricting to a single element r_k of $\boldsymbol{F}_{\mathbf{C}}(\mathcal{G})$, we can model its final value as the binomially distributed random variable $r_k \sim \frac{1}{n}\mathrm{Bin}\left(n, \gamma\omega_k\right)$. As a consequence of the Chernoff bound (cf. Corollary B.1), and that $\delta_k < \omega_k$, we have

$$\Pr\left[\left|r_k - \gamma\omega_k\right| \geq \gamma\delta_k\right] \leq 2\mathrm{e}^{-\frac{\gamma\delta_k^2 n}{3\omega_k}}.$$

Applying this bound to each element of the sum individually, we arrive at the desired result. □

Remark 3.1: The completeness error in the above lemma only considers the possibility of the protocol aborting during the parameter estimation stage. However, if the initial random seed is a particularly limited resource then it is possible that the protocol aborts due to seed exhaustion. In Lemma B.4 we analyse a sampling algorithm required to select the inputs during device interaction. If required, the probability of failure for that algorithm could be incorporated into the completeness error.

With a secure bound on the quantity of accumulated entropy established by Lemma 3.3 we can apply a $(k, \epsilon_{\text{ext}} + 2\epsilon_s)$-strong extractor to **AB** to complete the security analysis. Combined with the input randomness discussed in Appendix B we arrive at the following theorem.

Lemma 3.5 (Soundness of Protocol QRE)**:** *Let Protocol QRE be implemented with some initial random seed D of length d. Furthermore let all other protocol parameters be chosen within their permitted ranges, as detailed in Fig. 2. Then the soundness error of Protocol QRE is*

$$\varepsilon_{\text{sound}} = \max(\epsilon_{\text{ext}} + 2\epsilon_s, \epsilon_{\text{EAT}})\,.$$

Proof. Recall from (13) that the soundness error is an upper bound on $\frac{1}{2}\Pr[\Omega] \cdot \|\rho_{ZE} - \tau_m \otimes \rho_E\|_1$. In the case $\Pr[\Omega] \leq \epsilon_{\text{EAT}}$, we have $\frac{1}{2}\Pr[\Omega] \cdot \|\rho_{ZE} - \tau_m \otimes \rho_E\|_1 \leq \epsilon_{\text{EAT}}$.

In the case $\Pr[\Omega] > \epsilon_{\text{EAT}}$, Lemma 3.3 gives a bound on the accumulated entropy. Combining with the definition of a quantum-proof strong extractor Def. 2.5 and noting that the norm is non-increasing under partial trace we obtain $\frac{1}{2}\Pr[\Omega] \cdot \|\rho_{ZE} - \tau_m \otimes \rho_E\|_1 \leq \epsilon_{\text{ext}} + 2\epsilon_s$, from which the claim follows. □

Remark 3.2: By choosing parameters such that $\epsilon_{\text{EAT}} \leq \epsilon_{\text{ext}} + 2\epsilon_s$ we can take the soundness error to be $\epsilon_{\text{ext}} + 2\epsilon_s$.

Combining all of the previous results we arrive at the full security statement concerning Protocol QRE.

Theorem 3.1 (Security of Protocol QRE)**:** *Protocol QRE is an $(\varepsilon_{\text{comp}}, \varepsilon_{\text{sound}})$-secure randomness expansion protocol producing*

$$\left((1-\gamma)\left(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\boldsymbol{\lambda}_{\boldsymbol{\nu}} \cdot (\boldsymbol{\omega} - \boldsymbol{\delta}_{\text{sgn}})\right) - \epsilon_V - \epsilon_K\right) n - \epsilon_\Omega - \ell_{\text{ext}} \tag{38}$$

random bits at least $\varepsilon_{\text{sound}}$-close to uniformly distributed, where $\varepsilon_{\text{comp}}$, $\varepsilon_{\text{sound}}$ are given by Lemma 3.4 (cf. Remark 3.1) and Lemma 3.5.

Remark 3.3: The expected seed length required to execute Protocol QRE is $d \approx (\gamma H(\mu) + h(\gamma))\, n$ (cf. Lemma B.4).

Example 3.3: In Ex. 3.1 and Ex. 3.2 we used the following choice of protocol parameters: $n = 10^{10}$, $\gamma = 5 \times 10^{-3}$, $\delta_1 = \cdots = \delta_{|\mathcal{G}|} = 10^{-3}$ and $\epsilon_s = \epsilon_{\text{EAT}} = 10^{-8}$. The resulting implementation of Protocol QRE, using the nonlocal game $\mathcal{G}_{\text{CHSH}}$ with an expected frequency distribution $\boldsymbol{\omega} = (0.49, 0.4225, 0.0875)$, exhibits the following statistics.

Quantity	**Value**
Total accumulated entropy before extraction (no abort)	9.46×10^9
Expected length of required seed before extraction	5.54×10^8
Expected net-gain in entropy (no abort)	$8.91 \times 10^9 - \ell_{\text{ext}}$
Completeness error ($\varepsilon_{\text{comp}}$)	8.77×10^{-8}

4 Examples

In this section we demonstrate the use of our framework through the construction and analysis of several protocols based on different tests of nonlocality. To this end, we begin by introducing two families of nonlocal games which we consider alongside $\mathcal{G}_{\text{CHSH}}$.

Empirical behaviour game ($\mathcal{G}_{\text{EB}}$)**.** The *empirical behaviour game* ($\mathcal{G}_{\text{EB}}$) is a nonlocal game that estimates the underlying behaviour of $\mathfrak{D}_{AB}$, i.e., it attempts to characterise each individual probability $p(a,b|x,y)$. We may construct this by associating with each input-output tuple $(a,b,x,y) \in \mathcal{AB}\mathcal{X}\mathcal{Y}$ a corresponding score $c_{abxy} \in \mathcal{G}$ and defining the scoring rule

$$V_{\text{EB}}(a,b,x,y) := c_{abxy},$$

for each $(a,b,x,y) \in \mathcal{AB}\mathcal{X}\mathcal{Y}$. Then, for any input distribution μ_{EB} with full support on the alphabets $\mathcal{X}\mathcal{Y}$, the collection $\mathcal{G}_{\text{EB}} = (\mu_{\text{EB}}, V_{\text{EB}})$ forms a nonlocal game. Moreover, for agents playing according to some strategy $\boldsymbol{p} \in \mathcal{Q}$, the expected frequency distribution over the scores is precisely the joint distribution,

$$\begin{aligned}\omega_{\text{EB}}(a,b,x,y) &= \mu_{\text{EB}}(x,y)p(a,b|x,y)\\ &= p(a,b,x,y).\end{aligned}$$

As $\mathcal{G}_{\text{EB}}$ can be defined for any collection of input-output alphabets, we can indicate the size of these alphabets as superscripts, i.e., $\mathcal{G}_{\text{EB}}^{|\mathcal{X}||\mathcal{Y}||\mathcal{A}||\mathcal{B}|}$. However, since we only consider binary output alphabets in this work, we will not include their sizes in the superscript, i.e., we will write $\mathcal{G}_{\text{EB}}^{23}$ instead of $\mathcal{G}_{\text{EB}}^{2322}$.

Remark 4.1: The scoring rule for $\mathcal{G}_{\text{EB}}$, as defined above, has several redundant components, arising from normalisation and the no-signalling conditions. In fact, there are only $[(|\mathcal{A}|-1)|\mathcal{X}|+1][(|\mathcal{B}|-1)|\mathcal{Y}|+1]-1$ free parameters [51]. Knowing this we can reduce the number of scores in our nonlocal game and, in turn, the number of constraints we impose in our SDPs.[16]

Joint correlators game ($\mathcal{G}_{\langle AB\rangle}$). Specifically, for each $(x,y)\in\mathcal{X}\mathcal{Y}$ we define a score c_{xy} and a scoring rule

$$V_{\langle AB\rangle}(a,b,x,y) := \begin{cases} c_{xy} & \text{if } a=b \\ c_{\text{norm}} & \text{otherwise.} \end{cases}$$

That is, for a pair of inputs (x,y) the score is recorded as c_{xy} whenever the agents' outcomes agree. Otherwise, they record some normalization score c_{norm}. The input distribution can then be specified in some way: we use the uniform distribution over $\mathcal{X}\mathcal{Y}$. We refer to this game by the symbol $\mathcal{G}_{\langle AB\rangle}$ and, as before, we will indicate the sizes of the input alphabets with superscripts.

4.1 Rates in the presence of inefficient detectors

We now compare the accumulation rates of protocols built using the nonlocal games described above. We retain the protocol parameter choices from the previous examples: $n=10^{10}$, $\gamma=5\times10^{-3}$ and $\epsilon_s=\epsilon_{\text{EAT}}=10^{-8}$, except we now set the confidence interval width parameter to

$$\delta_k=\sqrt{\frac{3\,\omega_k\ln(2/\varepsilon_{\text{comp}})}{\gamma n}}, \tag{39}$$

in order to have a similar completeness error $\varepsilon_{\text{comp}}\approx10^{-12}$ across the different protocols.[17]

We suppose that the devices operate by using a pure, entangled state of the form

$$|\psi(\theta)\rangle_{AB}=\cos(\theta)\,|00\rangle+\sin(\theta)\,|11\rangle\,, \tag{40}$$

for $\theta\in(0,\pi/4]$. We denote the corresponding density operator by $\rho_\theta=|\psi(\theta)\rangle\langle\psi(\theta)|$. For simplicity we restrict to projective measurements within the x-z plane of the Bloch-sphere, i.e., measurements $\{\Pi(\varphi),\mathbb{1}-\Pi(\varphi)\}$, with the projectors defined by

$$\Pi(\varphi)=\begin{pmatrix}\cos^2(\varphi/2) & \cos(\varphi/2)\sin(\varphi/2)\\ \cos(\varphi/2)\sin(\varphi/2) & \sin^2(\varphi/2)\end{pmatrix} \tag{41}$$

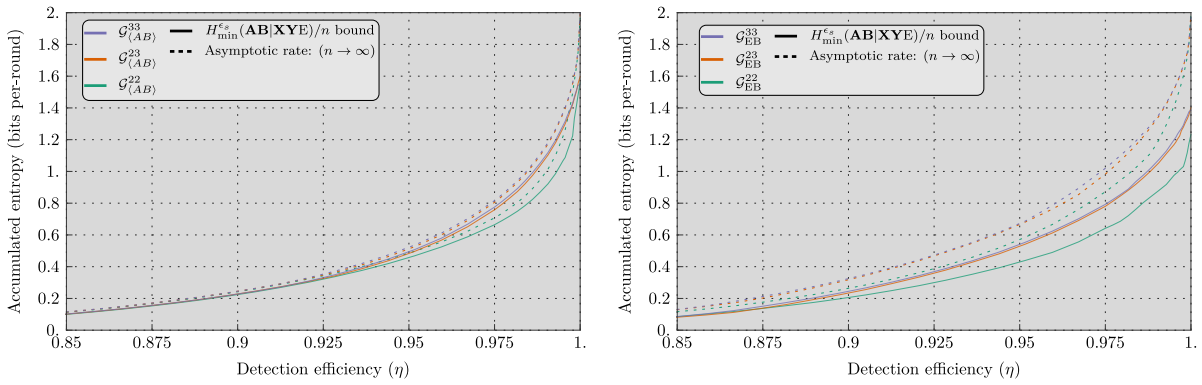
for $\varphi\in[0,2\pi)$. We denote the projectors associated with the j^{th} outcome of the i^{th} measurement by $A_{j|i}$ and $B_{j|i}$. The elements of the devices' behaviour can then be written as

$$p(a,b|x,y)=\text{Tr}\left[\rho_\theta(A_{a|x}\otimes B_{b|y})\right]. \tag{42}$$

Our analysis is focussed on how the accumulation rates differ when the devices operate with inefficient detectors. Heralding can be used to account for losses incurred during state transmission and has been used to develop novel device-independent protocols [52]. However, losses that occur within a user's laboratory cannot be ignored without opening a detection loophole [53]. Inefficient detectors are a major contributor to the total experimental noise, so robustness to inefficient detectors is a necessary property for any practical randomness expansion protocol. We characterize detection efficiency by a single parameter $\eta\in[0,1]$, representing the (independent) probability with which a measurement device successfully measures a received

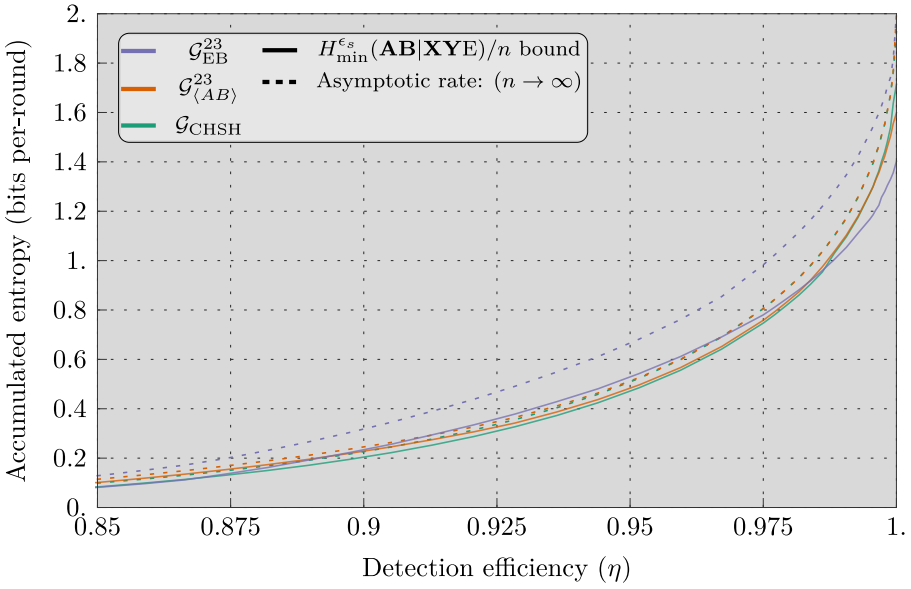
[16] It is important to remove redundant constraints in practice as they can lead to numerical instabilities.

[17] In practice one would fix the soundness error of the protocol. However, because the soundness error is also dependent on the extraction phase we instead assume independence of rounds and fix the completeness error.



(a) $\mathcal{G}_{\langle AB\rangle}$ protocols

(b) $\mathcal{G}_{\mathrm{EB}}$ protocols



(c) Comparison of protocols in the $(2,3)$-scenario.

Figure 5: A plot of the asymptotic and EAT-rates for protocols using the nonlocal game families $\mathcal{G}_{\langle AB\rangle}$, $\mathcal{G}_{\mathrm{EB}}$ and $\mathcal{G}_{\mathrm{CHSH}}$.

state and outputs the result.[18] To deal with failed measurements we assign outcome 0 when this occurs. Combining this with (42), we may write the behaviour as

$$\begin{aligned} p(a,b|x,y) = \eta^2 \mathrm{Tr}\left[\rho_\theta (A_{a|x}\otimes B_{b|y})\right] + (1-\eta)^2\delta_{0a}\delta_{0b} \\ + \eta(1-\eta)\left(\delta_{0a}\mathrm{Tr}\left[\rho_\theta(\mathbb{1}\otimes B_{b|y})\right] + \delta_{0b}\mathrm{Tr}\left[\rho_\theta(A_{a|x}\otimes\mathbb{1})\right]\right). \end{aligned} \tag{43}$$

For each protocol we consider lower bounds on two quantities: the pre-EAT gain in min-entropy from a single interaction, $H_{\min}(AB|XYE)$, and the *EAT-rate*, $H^{\epsilon_s}_{\min}(\mathbf{AB}|\mathbf{XYE})/n$. The former quantity, which we refer to as the *asymptotic rate*, represents the maximum accumulation rate achievable with our numerical technique. It is a lower bound on $H^{\epsilon_s}_{\min}(\mathbf{AB}|\mathbf{XYE})/n$, specified by (33), as $n\to\infty$ and $\gamma,\delta\to 0$.[19] Comparing these two quantities gives a clear picture of the amount of entropy that we lose due to the effect of finite statistics.

[18] For simplicity, we make the additional assumption that the detection efficiencies are constant amongst all measurement devices used within the protocol.

[19] We would really like to plot $H(AB|XYE)$ and the corresponding EAT-rate derived from it. However, in general we do not have suitable techniques to access these quantities in a device-independent manner.

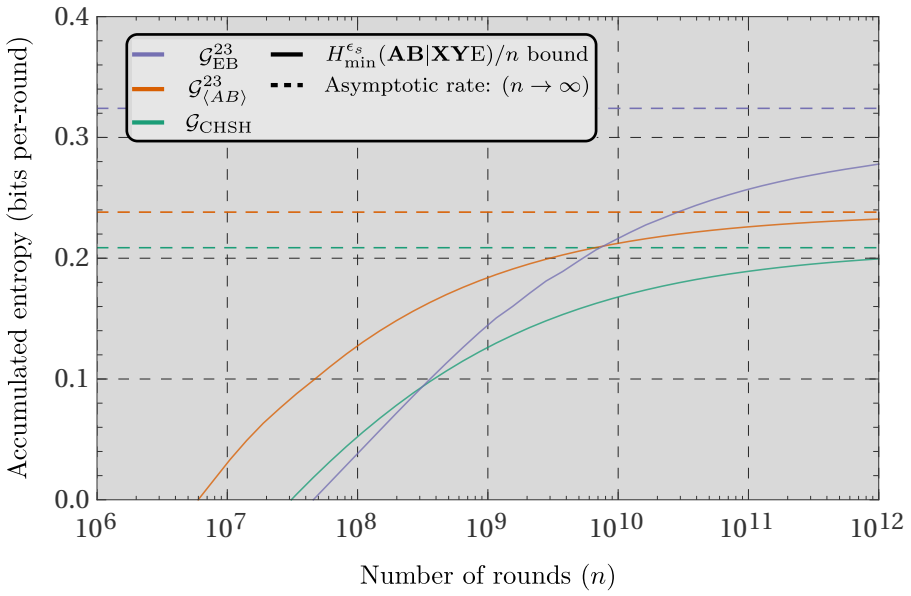


Figure 6: Comparison illustrating the EAT-rates (cf. (33)) converging to the asymptotic rates for protocols based on different nonlocal games. The rates were derived by assuming a qubit implementation of the protocols with a detection efficiency $\eta = 0.9$, optimizing the state and measurement angles in order to maximise the asymptotic rate. Then, for each value of n we optimized the min-tradeoff function choice and β parameter and noted the resulting bound on $H^{\epsilon_s}_{\min}$. To ensure that we approach the asymptotic rate as n increased we set $\gamma = \delta_1 = \cdots = \delta_{|\mathcal{G}|} = n^{-1/3}$, resulting in a constant completeness error across all values of n.

With inefficient detectors, partially entangled states can exhibit larger Bell-inequality violations than maximally entangled states [54]. To account for this we optimize both the state and measurement angles at each data point using the iterative optimization procedure detailed in [55]. All programs were relaxed to the second level of the NPA hierarchy using [56] and the resulting SDPs were computed using the SDPA solver [57]. The results of these numerics are displayed in Fig. 5.

In Fig. 5a and Fig. 5b we see that in both families of protocols considered, an increase in the number of inputs leads to higher rates. This increase is significant when one moves from the $(2, 2)$-scenario to the $(2, 3)$-scenario. However, continuing this analysis for higher numbers of inputs we find that any further increases appear to have negligible impact on the overall robustness of the protocol.[20] Whilst all of the protocols achieve asymptotic rates of 2 bits per round when $\eta = 1$, their respective EAT-rates at this point differ substantially. In Fig. 5c we see a direct comparison between protocols from the different families. The plot shows that, as expected, entropy loss is greater when using the nonlocality test G^{23}_{EB} as opposed to the other protocols. In particular, for high values of η we find that we would be able to certify a larger quantity of entropy by considering fewer scores. However, it is still worth noting that this entropy loss could be reduced by choosing a more generous set of protocol parameters, e.g., increasing n and decreasing δ.

Increasing n can be difficult in practice due to restrictions on the overall runtime of the protocol. Not only does it take longer to collect the statistics within the device-interaction phase, but it may also increase the runtime of the extraction phase [58]. In Fig. 6 we observe how quickly the various protocols converge on their respective asymptotic rates as we increase n. Again we find that, due to the finite-size effect, entropy loss when using $\mathcal{G}^{23}_{\mathrm{EB}}$ is greater than that observed in the other protocols. In particular, we see that for protocols with fewer than 10^{10} rounds, it is advantageous to use $\mathcal{G}^{23}_{\langle AB\rangle}$. From the perspective of practical implementation, Fig. 5c and Fig. 6 highlight the benefits of a flexible protocol framework wherein a user can design protocols tailored to the scenario under consideration.

[20] This could also be an artefact of the assumed restriction to qubit systems.

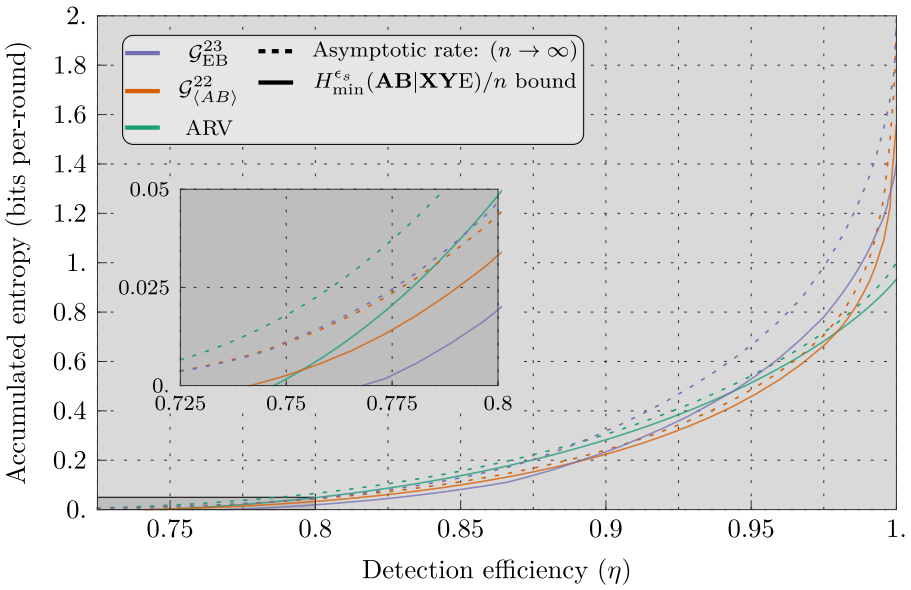


Figure 7: Comparison between the certifiable accumulation rates of QRNE protocols based on $\mathcal{G}_{\mathrm{CHSH}}$, $\mathcal{G}^{23}_{\mathrm{EB}}$ and Protocol ARV from [14] on qubit systems with inefficient detectors (cf. Fig. 5). The rates of Protocol ARV are also evaluated using the improved EAT statement [23]. For Protocol ARV, we use the one-sided von Neumann entropy bound, so the maximum rate is one bit per round, but because we can directly get the single-round von Neumann entropy, the rate initially falls more slowly with decreasing detection efficiency than for the other protocols.

It is also important to compare the rates of instances of Protocol QRE with other protocols from the literature, in particular the protocol of [14] (ARV). In [14], the min-tradeoff functions are constructed from a tight bound on the single-party von Neumann entropy, $H(A|XE)$, which is given in terms of a CHSH inequality violation [35]. In Fig. 7 we compare the rates of ARV with $\mathcal{G}^{22}_{\langle AB\rangle}$ and $\mathcal{G}^{23}_{\mathrm{EB}}$ for entangled qubit systems with inefficient detectors. To make our comparison fair, we have also computed the rates for Protocol ARV using the improved EAT bound[21]. As the rates of Protocol ARV are derived from the entropy accumulated by a single party their rates are capped at one bit per round.

In contrast, the semidefinite programs grant us access to bounds on the entropy produced by both parties and we are therefore able to certify up to two bits per round. In Fig. 7, this advantage is observed in the high detection efficiency regime. Fig. 7 also highlights a significant drawback of our technique, which stems from our use of the inequality $H(AB|XYE) \geq H_{\min}(AB|XYE)$. In particular, we see that for $\eta < 0.9$, the $H(A|XE)$ bound for the CHSH inequality is already greater than the $H_{\min}(AB|XYE)$ established for the empirical behaviour. Therefore, in the asymptotic limit ($n \to \infty$) the min-entropy bounds for these protocols will produce strictly worse rates in this regime. For the finite n we have chosen, $n = 10^{10}$, it appears that for the majority of smaller η, it is advantageous to use the ARV protocol over the protocols derived from the framework. Nevertheless, looking at the threshold detection efficiencies, i.e. the minimal detection efficiency required to achieve positive rates, we find that some protocols from our framework are able to again beat the rates established for Protocol ARV. Looking at the inset plot in Fig. 7 we see that $\mathcal{G}^{22}_{\langle AB\rangle}$ has a smaller threshold efficiency than that of Protocol ARV for the chosen protocol parameters. Interestingly, this shows that $\mathcal{G}^{22}_{\langle AB\rangle}$ is capable of producing higher rates than Protocol ARV in both the low and the high detection efficiency regimes, with the improvement for low detection efficiencies being of particular relevance to experimental implementations. Importantly, this shows that protocols from the framework are of practical use for finite n in spite of the losses coming from the use of $H(AB|XYE) \geq H_{\min}(AB|XYE)$.

Remark 4.2: We have so far considered the only noise to be that caused by inefficient detectors. However, it is natural to ask how other sources of noise affect our results. By replacing the states used with Werner states [59], we find that the results remain robust—they remain qualitatively the same, but for small Werner state noise, all of the graphs shift to slightly lower rates. For this reason we choose not to include the graphs here.

5 Conclusion

We have shown how to combine device-independent bounds on the guessing probability with the EAT, to create a versatile method for analysing quantum-secure randomness expansion protocols. The construction was presented as a template protocol from which an exact protocol can be specified by the user. The relevant security statements and quantity of output randomness of the derived protocol can then be evaluated numerically. A Python package [24] accompanies this work to help facilitate implementation of the framework. In Sec. 4 we illustrated the framework, applying it to several example protocols, with parameters chosen to reflect the capabilities of current nonlocality tests. We then compared the robustness of these protocols when implemented on qubit systems with inefficient detectors. Our analyses show that, within a broadly similar experimental setup, different protocols can have significantly different rates, and hence that it is worth considering small modifications to a protocol during their design. We also compared the rates of a selection of our protocols to the protocol presented in [14] (ARV). Interestingly, we found that some of the protocols from the framework are able to achieve higher rates than Protocol ARV in both the high and low detection efficiency regimes. In particular, the higher rates for low detection efficiencies is of great importance for actual experimental implementations.

Although the framework produces secure and robust protocols, there remains scope for further improvements. For example, our work relies on the relation $H(AB|XYE) \geq H_{\min}(AB|XYE)$ which is far from tight. The resulting loss can be seen when one compares the asymptotic rate of $\mathcal{G}_{\mathrm{CHSH}}$ in Fig. 5c with those presented in [14] (see Fig. 7). Several alternative approaches could be taken in order to reduce this loss.

[21] Note that we always use the direct bound on the von Neumann entropy when considering Protocol ARV, rather than forming a bound via the min-entropy

Firstly, the above relation is part of a more general ordering of the conditional Rényi entropies.[22] If one were able to develop efficient computational techniques for computing device-independent lower bounds on one of these alternative quantities we would expect an immediate improvement. Furthermore, dimension-dependent bounds may be applicable in certain situations. For example, it is known that for the special case of n-party, 2-input, 2-output scenarios it is sufficient to restrict to qubit systems [35, 51].

Optimizing the choice of min-tradeoff function over $\mathcal{F}_{\min}$ is a non-convex and not necessarily continuous problem [60]. Our analysis in Sec. 4 used a simple probabilistic gradient ascent algorithm to approach this problem. We found that for certain protocols, in particular $\mathcal{G}^{22}_{\text{EB}}$, the optimization had to be repeated many times before a good choice of min-tradeoff function was found.

As Fig. 7 shows, the framework is capable of producing protocols that are of immediate relevance to current randomness expansion experiments. It is therefore a worthwhile endeavour to search for protocols within the framework that provide high EAT-rates in different parameter regimes. Investigations into the randomness certification properties of nonlocality tests with larger output alphabets or additional parties could be of interest. However, increasing either of these parameters is likely to increase the influence of finite-size effects. Alternatively, one could try to design more economical nonlocality tests by combining scores that are of a lesser importance to the task of certifying randomness. Intuitively, for a score $c \in \mathcal{C}$, the magnitude of of $\lambda(c)$ in the min-tradeoff function indicates how important that score is for certifying entropy. If $|\lambda(c)|$ is large then this score is 'important' in the sense that any small deviations in the expected frequency of that score, $\omega(c)$, will have a large impact on the amount of certifiable entropy. Another approach to designing good nonlocality tests would be to take inspiration from [20, 21] wherein the authors showed how to derive the optimal Bell-expressions for certifying randomness. A nonlocal game could then be designed to encode the constraints imposed by this optimal Bell-expression. An example of such a game would be to assign a score $+1$ to all $(ABXY)$ that have a positive coefficient in the optimal Bell-expression and a score of -1 to all those with negative coefficients. The input distribution of the nonlocal game could then be chosen as such to encode the relative weights of the coefficients.

Finally, our computational approach to the EAT considered only the task of randomness expansion. Our work could be extended to produce security proofs for other device-independent tasks. Given that the EAT has already been successfully applied to a wide range of problems [36, 62–65], developing good methods for robust min-tradeoff function constructions represents an important step towards practical device-independent security.

Acknowledgments

We are grateful for support from the EPSRC's Quantum Communications Hub (grant number EP/M013472/1), an EPSRC First Grant (grant number EP/P016588/1) and the WW Smith fund.

References

[1] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, "Mining your Ps and Qs: Detection of widespread weak keys in network devices," in *Proceedings of the 21st USENIX Security Symposium*, Aug. 2012.

[2] P. Chaiwongkhot, S. Sajeed, L. Lydersen, and V. Makarov, "Finite-key-size effect in a commercial plug-and-play QKD system," *Quantum Science and Technology*, vol. 2, no. 4, p. 044003, 2017.

[3] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS-98)*, (Los Alamitos, CA, USA), pp. 503–509, IEEE Computer Society, 1998.

[4] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[22] The Rényi entropies are one of many different entropic families that include the von Neumann entropy as a limiting case. Any such family could be used if they satisfy an equivalent relation.

[5] R. Colbeck, *Quantum and Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2007. Also available as `arXiv:0911.3814`.

[6] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," *Journal of Physics A*, vol. 44, no. 9, p. 095305, 2011.

[7] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, pp. 1021–1024, 2010.

[8] S. Pironio and S. Massar, "Security of practical private randomness generation," *Physical Review A*, vol. 87, p. 012336, 2013.

[9] S. Fehr, R. Gelles, and C. Schaffner, "Security and composability of randomness expansion from Bell inequalities," *Physical Review A*, vol. 87, p. 012335, 2013.

[10] C. A. Miller and Y. Shi, "Universal security for randomness expansion from the spot-checking protocol," *arXiv preprint arXiv:1411.6608*, 2014.

[11] C. A. Miller and Y. Shi, "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices," in *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, (New York, NY, USA), pp. 417–426, ACM, 2014.

[12] U. Vazirani and T. Vidick, "Certifiable quantum dice or, testable exponential randomness expansion," in *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC-12)*, pp. 61–76, 2012.

[13] F. Dupuis, O. Fawzi, and R. Renner, "Entropy accumulation." e-print `arXiv:1607.01796`, 2016.

[14] R. Arnon-Friedman, R. Renner, and T. Vidick, "Simple and tight device-independent security proofs." *SIAM Journal on Computing*, vol. 48, no. 1, pp. 181225, 2019.

[15] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," *Nature communications*, vol. 9, no. 1, p. 459, 2018.

[16] E. Knill, Y. Zhang, and H. Fu, "Quantum probability estimation for randomness with quantum side information." e-print `arXiv:1806.04553`, 2018.

[17] O. Nieto-Silleras, C. Bamps, J. Silman, and S. Pironio, "Device-independent randomness generation from several Bell estimators," *New Journal of Physics*, vol. 20, no. 2, p. 023049, 2018.

[18] M. Navascués, S. Pironio, and A. Acín, "Bounding the set of quantum correlations," *Physical Review Letters*, vol. 98, no. 1, p. 010401, 2007.

[19] M. Navascués, S. Pironio, and A. Acín, "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations," *New Journal of Physics*, vol. 10, no. 7, p. 073013, 2008.

[20] O. Nieto-Silleras, S. Pironio, and J. Silman, "Using complete measurement statistics for optimal device-independent randomness evaluation," *New Journal of Physics*, vol. 16, no. 1, p. 013035, 2014.

[21] J.-D. Bancal, L. Sheridan, and V. Scarani, "More randomness from the same data," *New Journal of Physics*, vol. 16, no. 3, p. 033011, 2014.

[22] R. König, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4337–4347, 2009.

[23] F. Dupuis and O. Fawzi, "Entropy accumulation with improved second-order," *IEEE Transactions on information theory*, 2019.

[24] "Python package for DI protocol development." `https://github.com/peterjbrown519/dirng`, 2018.

[25] P. Mironowicz and M. Pawowski. "Robustness of quantum-randomness expansion protocols in the presence of noise," *Physical Review A* vol. 88.3, p. 032319, 2013.

[26] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, "Significant-loophole-free test of Bells theorem with entangled photons," *Physical Review Letters* vol. 115, p. 250401, 2015.

[27] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellan, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, "Strong loophole-free test of local realism," *Physical Review Letters* vol. 115, p. 250402, 2015.

[28] B. Hensen, H. Bernien, A. E. Drau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abella, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," *Nature* vol. 526, pp. 682686, 2015.

[29] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, "Towards a realization of device-independent quantum key distribution," *arXiv preprint arXiv:1811.07983*, 2018.

[30] R. Renner, *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology, Zurich, 2005. Also available as `quant-ph/0512258`.

[31] R. Renner and S. Wolf, "Smooth Rényi entropy and applications," in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, p. 233, IEEE, 2004.

[32] M. Tomamichel, R. Colbeck, and R. Renner, "Duality between smooth min- and max-entropies," *IEEE Transactions on information theory*, vol. 56, no. 9, pp. 4674–4681, 2010.

[33] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*, vol. 5. Springer, 2015.

[34] E. Hänggi and R. Renner, "Device-independent quantum key distribution with commuting measurements." e-print `arXiv:1009.1833`, 2010.

[35] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Physical Review Letters*, vol. 98, p. 230501, 2007.

[36] M. Kessler and R. Arnon-Friedman, "Device-independent randomness amplification and privatization," *arXiv preprint arXiv:1705.04148*, 2017.

[37] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality," *Reviews of Modern Physics*, vol. 86, no. 2, p. 419, 2014.

[38] S. Popescu and D. Rohrlich, "Which states violate Bell's inequality maximally?," *Physics Letters A*, vol. 169, no. 6, pp. 411–414, 1992.

[39] R. Canetti, "Security and composition of multiparty cryptographic protocols," *Journal of Cryptology*, vol. 13, no. 1, pp. 143–202, 2000.

[40] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols.," in *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science (FOCS-01)*, pp. 136–145, 2001.

[41] B. Pfitzmann and M. Waidner, "A model for asynchronous reactive systems and its application to secure message transmission," in *Proceedings of the 2001 IEEE Symposium on Security and Privacy (SP01)*, (Washington, DC, USA), pp. 184–201, IEEE Computer Society, 2001.

[42] M. Ben-Or and D. Mayers, "General security definition and composability for quantum & classical protocols." e-print `quant-ph/0409062`, 2004.

[43] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," *arXiv preprint arXiv:1409.3525*, 2014.

[44] J. Barrett, R. Colbeck, and A. Kent, "Memory attacks on device-independent quantum cryptography," *Physical Review Letters*, vol. 106, p. 010503, 2013.

[45] M. Tomamichel, R. Colbeck, and R. Renner, "A fully quantum asymptotic equipartition property," *IEEE Transactions on information theory*, vol. 55, no. 12, pp. 5840–5847, 2009.

[46] M. Ledoux, *The concentration of measure phenomenon*. American Mathematical Soc., 2005.

[47] A. De, C. Portmann, T. Vidick, and R. Renner, "Trevisan's extractor in the presence of quantum side information." e-print `arXiv:0912.5514`, 2009.

[48] R. Konig and R. Renner, "Sampling of min-entropy relative to quantum knowledge," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4760–4787, 2011.

[49] L. Trevisan, "Extractors and pseudorandom generators," *Journal of the ACM*, vol. 48, no. 4, pp. 860–879, 2001.

[50] N. Nisan and A. Ta-Shma, "Extracting randomness: A survey and new constructions," *J. Comput. Syst. Sci.*, vol. 58, no. 1, pp. 148–173, 1999.

[51] B. Tsirelson, "Some results and problems on quantum Bell-type inequalities," *Hadronic Journal Supplement*, vol. 8, pp. 329–345, 1993.

[52] A. Máttar, J. Kolodyński, P. Skrzypczyk, D. Cavalcanti, K. Banaszek, and A. Acín, "Device-independent quantum key distribution with single-photon sources," *arXiv preprint arXiv:1803.07089*, 2018.

[53] P. M. Pearle, "Hidden-variable example based upon data rejection," *Physical Review D*, vol. 2, no. 8, pp. 1418–1425, 1970.

[54] P. H. Eberhard, "Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment," *Physical Review A*, vol. 47, pp. 747–750, 1993.

[55] S. M. Assad, O. Thearle, and P. K. Lam, "Maximizing device-independent randomness from a Bell experiment by optimizing the measurement settings," *Physical Review A*, vol. 94, no. 1, p. 012304, 2016.

[56] P. Wittek, "Algorithm 950: Ncpol2sdpa - sparse semidefinite programming relaxations for polynomial optimization problems of noncommuting variables," *ACM Transactions on Mathematical Software (TOMS)*, vol. 41, no. 3, p. 21, 2015.

[57] K. Fujisawa, M. Kojima, K. Nakata, and M. Yamashita, "SDPA (semidefinite programming algorithm) users manual - version 6.2.0," *Department of Mathematical and Com-puting Sciences, Tokyo Institute of Technology. Research Reports on Mathematical and Computing Sciences Series B: Operations Research*, 2002.

[58] W. Mauerer, C. Portmann, and V. B. Scholz, "A modular framework for randomness extraction based on Trevisan's construction," *arXiv preprint arXiv:1212.0520*, 2012.

[59] R. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," *Physical Review A*, vol. 40, no. 8, p. 4277, 1989.

[60] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín, "Unbounded randomness certification using sequences of measurements," *Physical Review A*, vol. 95, no. 2, p. 020102, 2017.

[61] A. Acín, S. Massar, and S. Pironio, "Randomness versus nonlocality and entanglement," *Phys. Rev. Lett.*, vol. 108, p. 100402, Mar 2012.

[62] J. Ribeiro, G. Murta, and S. Wehner, "Fully device-independent conference key agreement," *Phys. Rev. A*, vol. 97, p. 022307, Feb 2018.

[63] J. Ribeiro, L. P. Thinh, J. Kaniewski, J. Helsen, and S. Wehner, "Device independence for two-party cryptography and position verification with memoryless devices," *Phys. Rev. A*, vol. 97, p. 062307, Jun 2018.

[64] R. Arnon-Friedman and J.-D. Bancal, "Device-independent certification of one-shot distillable entanglement," *arXiv preprint arXiv:1712.09369*, 2017.

[65] C. Bamps, S. Massar, and S. Pironio, "Device-independent randomness generation with sublinear shared quantum resources," *Quantum*, vol. 2, p. 86, 2018.

[66] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *The Annals of Mathematical Statistics*, vol. 23, no. 4, pp. 493–507, 1952.

[67] T. Hagerup and C. Rüb, "A guided tour of Chernoff bounds," *Information Processing Letters*, vol. 33, pp. 305–308, 1990.

[68] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963.

[69] T. S. Han and M. Hoshi, "Interval algorithm for random number generation," *IEEE Transactions on Information Theory*, vol. 43, no. 2, pp. 599–611, 1997.

[70] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley and Sons Inc., 2nd ed., 2006.

[71] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.

A Table of parameters and notation

Notation	Description	Initial reference
$\mathfrak{D}$	A collection of untrusted devices.	Section 2.3
$\mathcal{G}$	A nonlocal game.	Definition 2.1
$\mathcal{Q}_{\mathcal{G}}$	Set of expected frequency distributions on $\mathcal{G}$ using quantum strategies.	Section 2.3
$\mathcal{Q}_{\mathcal{G}}^{(k)}$	Set of expected frequency distributions on $\mathcal{G}$ using strategies from $\mathcal{Q}^{(k)}$.	Section 2.3
$\boldsymbol{\nu}, \boldsymbol{\omega}$	Expected frequency distributions over scores of a nonlocal game.	Equation 11
$p_{\text{guess}}^{(k)}$, $d_{\text{guess}}^{(k)}$	Solutions to the k-relaxed primal and dual guessing probability programs.	Program 9 and 10
$\boldsymbol{\lambda}_{\boldsymbol{\nu}}$	Feasible point of the dual guessing probability program with parameter $\boldsymbol{\nu}$.	Section 2.3
$\boldsymbol{\delta}$	Vector of statistical confidence interval widths.	Equation 16.
$\boldsymbol{\delta}_{\text{sgn}}$	$\boldsymbol{\delta}$ with elements signed in accordance with a given $\boldsymbol{\lambda}$.	Lemma 3.3
$\mathcal{A}, \mathcal{B}$	Devices' output alphabets.	Section 2.1
$\mathcal{X}, \mathcal{Y}$	Devices' input alphabets.	Section 2.1
$n \in \mathbb{N}$	Number of rounds in the device-interaction phase.	Section 2.5.1
$\gamma \in (0, 1)$	Probability that any given round is a test round.	Section 2.5.1
A_i, B_i	Devices' outputs for the i^{th} round.	Section 2.5.1
X_i, Y_i	Devices' inputs for the i^{th} round.	Section 2.5.1
C_i	EAT-score for the i^{th} round.	Section 2.5.1
$\boldsymbol{F}_{\mathbf{C}}$	Frequency distribution induced by score transcript $\mathbf{C} = (C_1, \ldots, C_n)$.	Equation 15
Ω	Event that the protocol does not abort.	Equation 16
R_{ext}	Strong quantum-secure randomness extractor.	Definition 2.5
$\varepsilon_{\text{comp}}$	Completeness error of Protocol QRE.	Lemma 3.4
$\varepsilon_{\text{sound}}$	Soundness error of Protocol QRE.	Lemma 3.5
ε_s	Smoothing parameter for $H_{\min}$.	Equation 7
ϵ_{EAT}	Tolerance of unlikely success events.	Lemma 3.3.
ϵ_V	EAT error term (Variance).	Theorem 2.1
ϵ_K	EAT error term (Remainder).	Theorem 2.1
ϵ_Ω	EAT error term (Pass probability).	Theorem 2.1
ϵ_{ext}	Extractor error.	Definition 2.5
ℓ_{ext}	Entropy lost during extraction.	Section 2.6

B Input Randomness

Here we quantify the length of the initial random seed required to execute an instance of Protocol QRE. This supply of random bits is necessary for selecting the devices' inputs and seeding the extractor. In the forthcoming analysis we ignore the latter as this quantity depends on the choice of extractor. Instead, we look at the process of converting a uniform private seed into device inputs required for running Protocol QRE. We follow a similar procedure to that used in [14], modifying the algorithm slightly in order to extract explicit bounds.

B.1 Statistical bounds

We begin by stating some standard statistical bounds. The first is commonly known as the Chernoff bound [66], although we take our formulation from [67]. This provides a convenient bound on the deviation of the sum of random variables from the expected value.

Lemma B.1 (Chernoff bound)**:** *Let X_i be independent binary random variables for $i = 1, \ldots, n$, $S = \sum_i X_i$ and $\mu = \mathbb{E}[S]$. Then for $0 \leq t \leq 1$*

$$\Pr[S \geq (1+t)\mu] \leq \mathrm{e}^{-t^2\mu/3}$$
$$\Pr[S \leq (1-t)\mu] \leq \mathrm{e}^{-t^2\mu/2}.$$

Corollary B.1: *For $r \leq \mu$ we have* $\Pr[|S - \mu| \geq r] \leq 2\mathrm{e}^{-r^2/(3\mu)}$.

In addition to this, we also make use of Hoeffding's inequality [68].

Lemma B.2 (Hoeffding's inequality)**:** *Let X_i be independent random variables, such that $a_i \leq X_i \leq b_i$ with $a_i, b_i \in \mathbb{R}$ for $i = 1, \ldots, n$. In addition, let $S = \sum_i X_i$ and $\mu = \mathbb{E}[S]$. Then for $t > 0$*

$$\Pr[|S - \mu| \geq t] \leq 2\mathrm{e}^{-\frac{2t^2}{\sum_i (b_i - a_i)^2}}$$

B.2 Rounded interval algorithm

The interval algorithm provides an efficient method for simulating the sampling of some target random variable T using another random variable S. To aid understanding of our modification to this algorithm and any subsequent results we shall briefly explain how this simulation works. For simplicity we restrict ourselves to the scenario where S is a sequence of uniformly distributed bits, we denote the uniform distribution on an alphabet of size 2^k by U_{2^k}, for $k \in \mathbb{N}$.

The distribution of the target random variable T forms a partition of the unit interval, one subinterval for each outcome t of T. In exactly the same way, the probability distribution for U_{2^k} partitions the unit interval into 2^k subintervals. Thus, we can associate a bit-string with its corresponding subinterval, defined by this partitioning. The interval algorithm works by using an increasing sequence of random bits and the corresponding subintervals that the sequence defines. Once the subinterval generated by the sequence of bits is contained inside one of the subintervals defined by the target random variable T, say t, then we say that we have simulated the sampling of t from T and the algorithm terminates. Denoting by N the length of seed required for the interval algorithm to terminate, then by [69, Theorem 3] we have

$$\mathbb{E}[N] \leq H(T) + 3. \tag{44}$$

As the algorithm stands, the maximum value that N can take is unbounded (although the probability that the algorithm expends the seed without terminating decreases exponentially in N). In order to produce large deviation bounds on the number of bits required to execute our protocol, we place an upper limit on the maximum seed length. We thus use an adapted sampling procedure, the *rounded interval algorithm* (RIA), which forcefully terminates if the seed length reaches the upper bound of $k_{\max}$ bits.

Should the RIA fail to terminate after $k_{\max}$ steps, then the output sequence generated will correspond to some subinterval $I(r) = [\frac{r}{2^{k_{\max}}}, \frac{r+1}{2^{k_{\max}}})$, for some $r \in \{0, 1, \ldots, 2^{k_{\max}} - 1\}$, that is not entirely contained within one of the subintervals induced by T. If this occurs, we *round down*: selecting the interval I_t for which $\frac{r}{2^{k_{\max}}} \in I_t$.

Remark B.1: Note that the above procedure depends on the ordering of the intervals generated by T (which should be fixed before sampling). One could imagine a rather pathological scenario where an ordering places extremely unlikely outcomes over rounding points, greatly increasing their simulated outcome probabilities. However, as will be shown in Lemma B.3, the distance between the simulated random variable and the target random variable decreases exponentially in $k_{\max}$.

Remark B.2: The rounding procedure truncates the maximum seed length, $N \leq k_{\max}$, and as such, it is clear that the inequality (44) also holds for the RIA.

Definition B.1 (Statistical distance)**:** Given two random variables X and X', taking values in some common alphabet $\mathcal{X}$. The *statistical distance* between X and X', is defined by

$$\Delta(X, X') := \frac{1}{2} \sum_{x \in \mathcal{X}} |p_X(x) - p_{X'}(x)|. \tag{45}$$

Lemma B.3: *Let T be a random variable taking values in some alphabet $\mathcal{T}$. Let T' be the distribution sampled using the RIA with target distribution T. Then*

$$\Delta(T, T') \leq |\mathcal{T}|\, 2^{-(k_{\max}+1)},$$

where $k_{\max}$ is the maximum number of input bits that can be used by the RIA.

Proof. Consider the partitions of the unit interval $\{I(t)\}_{t\in\mathcal{T}}$ and $\{I'(t)\}_{t\in\mathcal{T}}$ corresponding to the distributions p_T and $q_{T'}$ of T and T' respectively. The intervals of T' take the form

$$I'(t) = \bigcup_r \left[\frac{r}{2^{k_{\max}}}, \frac{r+1}{2^{k_{\max}}}\right)$$

where the (potentially empty) union is taken over all $r \in \mathbb{N}_0$ such that $r2^{-k_{\max}} \in I(t)$. The intervals within the union are either contained fully within the corresponding outcome interval of T, i.e., $\left[\frac{r}{2^{k_{\max}}}, \frac{r+1}{2^{k_{\max}}}\right) \subseteq I(t)$, or they are included as a result of rounding. Thus we may write

$$|I'(t)| = |\{r \mid r \cdot 2^{-k_{\max}} \in I(t), r \in \mathbb{N}_0\}|2^{-k_{\max}}.$$

By a straightforward counting argument, there are at least $\left\lfloor |I(t)|2^{k_{\max}} \right\rfloor$ such values of r, and at most $\left\lceil |I(t)|2^{k_{\max}} \right\rceil$. We hence have

$$|I(t)|2^{k_{\max}} - 1 \leq |I'(t)|2^{k_{\max}} \leq |I(t)|2^{k_{\max}} + 1,$$

and therefore

$$|p_T(t) - p_{T'}(t)| \leq 2^{-k_{\max}},$$

holds for all $t \in \mathcal{T}$. Applying this bound to each term within the $\Delta(T, T')$ sum completes the proof. □

B.3 Input randomness for Protocol QRE

Following the structure of Protocol QRE, we look to use the RIA to sample the devices' inputs for each round. In adherence with the Markov-chain condition (Def. 2.3), the natural procedure would be to sample at the beginning of each round. However, in practice this requires a much larger seed: because of (44) and the property $H(T^n) = nH(T)$, by sampling the joint distribution the expected saving is about $3n$ bits compared to repeating a single sample n times. Fortunately, this joint sampling can be implemented while maintaining the Markov-chain condition. Within the assumptions of Protocol QRE we allow the honest parties access to a trusted classical computer, which would also contain some trusted data storage—we assume that the parties can record their outcome strings without leakage. Therefore, using their trusted classical computer, the honest parties perform the RIA: sampling the random variables (X_1^n, Y_1^n) and subsequently storing the outcome on the trusted classical computer's harddrive. Crucially, the assumption that the user can prevent unwanted communication between devices implies this can all be done without any information leaking to the untrusted devices. Then, at the beginning of round i, the inputs (X_i, Y_i) are sent from the classical computer to the respective devices. By conducting the protocol in this manner we retain the Markov chain conditions—the inputs are sampled independently of the devices and furthermore, when the devices produce their outputs for the i^{th} round they can only have knowledge of the inputs for this round and all previous.

Due to potential computational constraints and to permit large deviation bounds on the number of bits required we will not assume that all n rounds are sampled at once. Instead, we split the n rounds into at most $\lceil n/m \rceil$ blocks of size m and apply the RIA to sample the inputs of each block separately. For simplicity, we assume that $n/m \in \mathbb{N}$ and henceforth remove the ceiling function from the analysis.

Recall that for the i^{th} round, the user first uses T_i to decide whether the round is a test round, and, if so, they choose inputs according to the nonlocal game input distribution μ. Otherwise, if $T_i = 0$, they supply their devices with the fixed inputs $\tilde{x}$ and $\tilde{y}$. The probability mass function of joint random variables $X_iY_iT_i$, representing the i^{th} round's inputs, is therefore

$$\Pr\left[(X_i, Y_i, T_i) = (x_i, y_i, t_i)\right] = \begin{cases} \gamma\,\mu(x,y) & \text{for } (x_i, y_i, t_i) = (x, y, 1), \\ (1-\gamma) & \text{for } (x_i, y_i, t_i) = (\tilde{x}, \tilde{y}, 0) \\ 0 & \text{otherwise} \end{cases}. \tag{46}$$

Following (44), if M is the seed length required to sample one of the m blocks of rounds, then we have

$$\mathbb{E}\left[M\right] \leq \frac{(\gamma H(\mu) + h(\gamma))\, n}{m} + 3 \tag{47}$$

where $H(\mu)$ is the Shannon entropy of the distribution μ and $h(\cdot)$ is the binary entropy.

The following lemma gives a probabilistic bound on the total length of the random seed required to sample the inputs for the devices.[23]

Lemma B.4: *Let the parameters of Protocol QRE be as defined in Fig. 2 and let $k_{\max} \in \mathbb{N}$ be the maximum permitted seed length for an instance of the RIA. Then, with probability greater than $(1 - \epsilon_{\text{RIA}})$, we can use m instances of the RIA to simulate the sampling of every device input required to execute Protocol QRE with a uniform seed of length no greater than $N_{\max}$, where*

$$N_{\max} = 2\kappa \tag{48}$$

$$\epsilon_{\text{RIA}} = e^{-2\kappa^2/mk_{\max}^2} \tag{49}$$

and $\kappa = (\gamma H(\mu) + h(\gamma))\, n + 3m$. Moreover, the sampled distribution lies within a statistical distance of

$$\epsilon_{\text{dist}} = m\, 2^{n \log(\text{supp}(\mu)+1)/m - (k_{\max}+1)}, \tag{50}$$

from the target distribution, where $\text{supp}(\mu) := |\{(x, y) \in \mathcal{X}\mathcal{Y} \mid \mu(x, y) > 0\}|$.

Proof. Consider the sequence $(M_i)_{i=1}^m$ of i.i.d. random variables representing the number of random bits required to choose the inputs for the i^{th} block and the corresponding random sum $N = \sum_{i=1}^m M_i$. By (47), the expected number of bits required to select all of the inputs for the protocol can be bounded above by $\kappa = (\gamma H(\mu) + h(\gamma))\, n + 3m$. Using Hoeffding's inequality, we can bound the probability that N greatly exceeds this value,

$$\Pr[N \geq \kappa + t] \leq e^{-2t^2/mk_{\max}^2},$$

for some $t > 0$. Setting $t = \kappa$ this becomes

$$\Pr[N \geq 2\kappa] \leq e^{-2\kappa^2/mk_{\max}^2}.$$

Although κ is not exactly the expected value of N, which is the quantity appearing in Hoeffding's bound, the bound holds because $\kappa \geq \mathbb{E}[N]$.

It remains to bound the statistical distance between the sampled random variable $\mathbf{I}' = (\mathbf{X}', \mathbf{Y}', \mathbf{T}')$ and the target random variable $\mathbf{I} = (\mathbf{X}, \mathbf{Y}, \mathbf{T})$. For each block of rounds, the corresponding random variable $\mathbf{I}_i$ can take one of a possible $(\text{supp}(\mu) + 1)^{n/m}$ different values. Therefore, by Lemma B.3, we have for the i^{th} block of rounds

$$\begin{aligned}\Delta(\mathbf{I}_i, \mathbf{I}_i') &\leq (\text{supp}(\mu) + 1)^{n/m} 2^{-(k_{\max}+1)} \\ &= 2^{n \log(\text{supp}(\mu)+1)/m - (k_{\max}+1)}\end{aligned}$$

Since $\Delta(W, V)$ is a metric and hence satisfies the triangle inequality [70], the statistical distance between independently repeated samples can grow no faster than linearly, i.e., $\Delta(I^m, I'^m) \leq m\Delta(I, I')$. This completes the proof. □

C Incorporating the blocking procedure of [14]

The original statement of the entropy accumulation theorem [13] was released alongside an accompanying paper, [14], which detailed its application to security proofs of device-independent protocols. Within the appendix of [14] it was shown that one could increase the quantity of entropy certified by the original EAT by modifying the structure of the protocol. In particular, this demonstrated the original EAT statement's suboptimal dependence on the testing probability. In light of this, the authors of [23] improved the second order term of the EAT in order to account for this suboptimal dependence. In the sections that follow, we will look at how the modified protocol structure interacts with the improved EAT statement. We begin by showing how the family of min-tradeoff functions $\mathcal{F}_{\min}$ can be adapted to this structural change and then we show that the modified protocol structure provides no clear benefits when used with the improved EAT statement. In addition, we provide some comparison plots showing the accumulation rates achievable with the different structures and EAT statements. To clearly distinguish the different statements of the EAT, we shall indicate with the subscript $_{\text{DFR16}}$, quantities associated with the original EAT [13] and similarly we shall indicate with the subscript $_{\text{DF18}}$, quantities associated with the EAT with improved second-order [23].

[23] We do not include the extractor's seed here as its size will depend on the choice of extractor.

C.1 Construction

Let us briefly review the structural modification that was introduced in [14]. Instead of distinguishing the statistics from each interaction separately, rounds are grouped together to form *blocks*. The number of rounds within a block can vary: a new block begins when either a test-round occurs or when the maximum number of rounds permitted within a block, $s_{\max}$, is reached. On expectation there are $\bar{s} = \frac{1-(1-\gamma)^{s_{\max}}}{\gamma}$ rounds within a block. The device-interaction phase of the protocol concludes after some specified number of blocks $m \in \mathbb{N}$ have terminated. We shall use the superscripts ^{R} and ^{B} to indicate whether a quantity is concerned with the round-by-round or block structured protocols respectively.

The collected information is now defined at the level of blocks and not rounds. In particular, at the end of the i^{th} block the user records some tuple $(\mathbf{A}_i, \mathbf{B}_i, \mathbf{X}_i, \mathbf{Y}_i, C_i)$, where $(\mathbf{A}_i, \mathbf{B}_i, \mathbf{X}_i, \mathbf{Y}_i) \in \mathcal{A}^{s_{\max}}\mathcal{B}^{s_{\max}}\mathcal{X}^{s_{\max}}\mathcal{Y}^{s_{\max}}$ and the score's alphabet remains the same, $C_i \in \mathcal{G} \cup \{\perp\}$. The EAT-channels are also defined for each block and the entropy bounding property (cf. (17)) that the min-tradeoff functions must satisfy becomes

$$f^B_{\min}(\boldsymbol{p}) \leq \inf_{\sigma_{R_{i-1}R'}:\mathcal{N}_i(\sigma)_{\mathbf{C}_i}=\tau_{\boldsymbol{p}}} H(\mathbf{A}_i\mathbf{B}_i|\mathbf{X}_i\mathbf{Y}_iR')_{\mathcal{N}_i(\sigma)}, \tag{51}$$

for each $i \in [m]$. The set of distributions compatible with the protocol structure (cf. (18)) now take the form

$$\boldsymbol{p}^B = \begin{pmatrix} \gamma\bar{s}\boldsymbol{q} \\ (1-\gamma)^{s_{\max}} \end{pmatrix} \tag{52}$$

for $\boldsymbol{q} \in \mathcal{Q}_{\mathcal{G}}$.

Lemma C.1 (Blocked variant of Lemma 3.1)**:** *Let $g : \mathcal{P}_{\mathcal{G}} \to \mathbb{R}$ be an affine function satisfying*

$$g(\boldsymbol{q}) \leq \inf_{\sigma_{R_{i-1}R'}:\mathcal{N}_i^{\text{test}}(\sigma)_{C_i}=\tau_{\boldsymbol{p}}} H(\mathbf{A}_i\mathbf{B}_i|\mathbf{X}_i\mathbf{Y}_iR')_{\mathcal{N}_i(\sigma)} \tag{53}$$

for all $\boldsymbol{q} \in \mathcal{Q}_{\mathcal{G}}$. Then the function $f : \mathcal{P}_{\mathcal{G}\cup\{\perp\}} \to \mathbb{R}$, defined by its action on trivial distributions

$$\begin{aligned} f(\mathbf{e}_c) &= \text{Max}[g] + \frac{g(\mathbf{e}_c) - \text{Max}[g]}{\gamma\bar{s}}, \qquad \forall c \in \mathcal{G}, \\ f(\mathbf{e}_\perp) &= \text{Max}[g], \end{aligned}$$

is a min-tradeoff function for any EAT-channels implementing Protocol QRE^B. Furthermore, f satisfies the following properties:

$$\begin{aligned} \text{Max}[f] &= \text{Max}[g], \\ \text{Min}[f|_\Gamma] &\geq \text{Min}[g], \\ \text{Var}[f|_\Gamma] &\leq \frac{(\text{Max}[g] - \text{Min}[g])^2}{\gamma\bar{s}}. \end{aligned}$$

Proof. This follows from replicating the original proof [23] with the block channels decomposed into the testing and generation channels, $\mathcal{N}_i = \gamma\bar{s}\mathcal{N}_i^{\text{test}} + (1-\gamma\bar{s})\mathcal{N}_i^{\text{gen}}$. □

Lemma C.2 (Blocked min-tradeoff construction)**:** *Let $\mathcal{G}$ be a nonlocal game and $k \in \mathbb{N}$. For each $\boldsymbol{\nu} \in \mathcal{Q}_{\mathcal{G}}^{(k)}$, let $\boldsymbol{\lambda}_{\boldsymbol{\nu}}$ be some feasible point of Prog. (10). Furthermore, let $\lambda_{\max} = \max_{c\in\mathcal{G}} \lambda_{\boldsymbol{\nu}}(c)$ and $\lambda_{\min} = \min_{c\in\mathcal{G}} \lambda_{\boldsymbol{\nu}}(c)$. Then, for any set of EAT channels $\{\mathcal{N}_i\}_{i=1}^m$ implementing an instance of Protocol QRE^B with the nonlocal game $\mathcal{G}$, the set of functionals $F^B_{\min}(\mathcal{G}) = \{f_{\boldsymbol{\nu}}(\cdot) \mid \boldsymbol{\nu} \in \mathcal{Q}_{\mathcal{G}}^{(k)}\}$ forms a family of min-tradeoff functions, where $f_{\boldsymbol{\nu}} : \mathcal{P}_{\mathcal{C}} \to \mathbb{R}$ are defined by their actions on trivial distributions*

$$f_{\boldsymbol{\nu}}(\mathbf{e}_c) := (1-\gamma)\,\bar{s}\left(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\frac{\boldsymbol{\lambda}_{\boldsymbol{\nu}}\cdot\mathbf{e}_c - (1-\gamma\bar{s})\lambda_{\min}}{\gamma\bar{s}}\right) \quad \text{for } c \in \mathcal{G}, \tag{54}$$

and

$$f_{\boldsymbol{\nu}}(\mathbf{e}_\perp) := (1-\gamma)\,\bar{s}\,(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\,\lambda_{\min})\,, \tag{55}$$

where $A_{\boldsymbol{\nu}} = \frac{1}{\ln 2} - \log(\boldsymbol{\lambda}_{\boldsymbol{\nu}}\cdot\boldsymbol{\nu})$ and $B_{\boldsymbol{\nu}} = \frac{1}{\boldsymbol{\lambda}_{\boldsymbol{\nu}}\cdot\boldsymbol{\nu}\ln 2}$.

Moreover, these min-tradeoff functions satisfy the following identities.

- *Maximum:*
$$\mathrm{Max}[f_{\boldsymbol{\nu}}] = (1-\gamma)\bar{s}(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\,\lambda_{\min}) \tag{56}$$
- Γ-*Minimum:*
$$\mathrm{Min}[\,f_{\boldsymbol{\nu}}|_{\Gamma}] \geq (1-\gamma)\bar{s}(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\,\lambda_{\max}) \tag{57}$$
- Γ-*Variance:*
$$\mathrm{Var}[\,f_{\boldsymbol{\nu}}|_{\Gamma}] \leq \frac{(1-\gamma)^2\bar{s}B_{\boldsymbol{\nu}}^2(\lambda_{\max}-\lambda_{\min})^2}{\gamma} \tag{58}$$

Proof. The proof follows the same structure as the proof of Lemma 3.2. The only significant difference is the construction of the function $g : \mathcal{P}_{\mathcal{G}} \to \mathbb{R}$ satisfying (53) so we shall explain this part here. Following Appendix B of [14], by repeated application of the chain rule we may decompose a block's entropy as

$$H(\mathbf{A}_i\mathbf{B}_i|\mathbf{X}_i\mathbf{Y}_i\mathbf{T}_iR')_{\mathcal{N}_i(\sigma)} = \sum_{j=1}^{s_{\max}}(1-\gamma)^{j-1}H(A_{i,j}B_{i,j}|\mathbf{X}_i\mathbf{Y}_i,\mathbf{T}_{i,1}^{\,j-1}{=}\,\mathbf{0},\mathbf{T}_{i,j}^{\,s_{\max}}\mathbf{A}_{i,1}^{\,j-1}\mathbf{B}_{i,1}^{\,j-1}R'),$$

where $T_{i,j}$ is the random variable indicating whether a test occurred on the j^{th} round of the i^{th} block. Considering the individual terms within the sum, we can absorb the majority of the side information into some arbitrary quantum register E leaving us with terms of the form

$$(1-\gamma)^{j-1}H(A_{i,j}B_{i,j}|X_{i,j}Y_{i,j}T_{i,j}\mathrm{E}).$$

As before, we can use the inequality $H(A|B) \geq H_{\min}(A|B)$ and conditioning on $T_{i,j}$ to lower bound each term in the sum by the outputs of the semidefinite program,

$$\begin{aligned}
(1-\gamma)^{j-1}H(A_{i,j}B_{i,j}|X_{i,j}Y_{i,j}T_{i,j}\mathrm{E}) &= (1-\gamma)^{j-1}\Pr\left[T_{i,j}=0\right]H(A_{i,j}B_{i,j}|X_{i,j}=\tilde{x},Y_{i,j}=\tilde{y},T_{i,j}=0,\mathrm{E}) \\
&\quad + (1-\gamma)^{j-1}\Pr\left[T_{i,j}=1\right]H(A_{i,j}B_{i,j}|X_{i,j}Y_{i,j}T_{i,j}=1\ \mathrm{E}) \\
&\geq (1-\gamma)^{j}H(A_{i,j}B_{i,j}|\tilde{x}\,\tilde{y}\,\mathrm{E}) \\
&\geq (1-\gamma)^{j}H_{\min}(A_{i,j}B_{i,j}|\tilde{x}\,\tilde{y}\,\mathrm{E}) \\
&\geq -(1-\gamma)^{j}\log(\boldsymbol{\lambda}_{\boldsymbol{\nu}}\cdot\boldsymbol{\omega}_{i,j}),
\end{aligned}$$

where $\boldsymbol{\omega}_{i,j} \in \mathcal{Q}_{\mathcal{G}}$ is the expected frequency distribution over the games scores for round j of block i. Noting that $-\log(\cdot)$ of a linear function is convex, we can establish a bound on the entire block i through an application of Jensen's inequality

$$\begin{aligned}
(\gamma-1)\sum_{j=1}^{s_{\max}}(1-\gamma)^{j-1}\log(\boldsymbol{\lambda}_{\boldsymbol{\nu}}\cdot\boldsymbol{\omega}_{i,j}) &\geq \bar{s}(\gamma-1)\log\left(\boldsymbol{\lambda}_{\boldsymbol{\nu}}\cdot\frac{\sum_{j=1}^{s_{\max}}(1-\gamma)^{j-1}\boldsymbol{\omega}_{i,j}}{\bar{s}}\right) \\
&= \bar{s}(\gamma-1)\log\left(\boldsymbol{\lambda}_{\boldsymbol{\nu}}\cdot\boldsymbol{\omega}_{i}\right),
\end{aligned}$$

we have used the fact that $\sum_{j\in[s_{\max}]}(1-\gamma)^{j-1} = \bar{s}$ and that $\boldsymbol{\omega}_i = \frac{\sum_{j\in[s_{\max}]}\gamma(1-\gamma)^{j-1}\boldsymbol{\omega}_{i,j}}{\gamma\bar{s}}$ is the normalised expected frequency distribution over the nonlocal game scores for the i^{th} block. Taking a first-order expansion of the last line, we get the function $g_{\boldsymbol{\nu}}(\,\cdot\,) = (1-\gamma)\bar{s}\,(A_{\boldsymbol{\nu}} - B_{\boldsymbol{\nu}}\boldsymbol{\lambda}_{\boldsymbol{\nu}}\cdot(\,\cdot\,))$. The proof is then completed by applying the extension Lemma C.1, analogous to the technique of Lemma 3.2. □

C.2 Blocking with the improved second order

The error term in the original EAT bound is

$$\epsilon_{\mathrm{DFR16}}^{R} := 2\left(\log(1+2|\mathcal{A}||\mathcal{B}|) + \lceil\|\nabla f_{\min}\|_{\infty}\rceil\right)\sqrt{1-2\log(\epsilon_s\epsilon_{\mathrm{EAT}})}. \tag{59}$$

The disadvantage of using this bound as-is is that the gradient of $f_{\min}$ scales like $1/\gamma$ and so the total error scales as $O(\sqrt{n}/\gamma)$. Collating the statistics into $m \in \mathbb{N}$ blocks, allows some of the γ dependence from the gradient term to be transferred to the $\log(1+2|\mathcal{A}||\mathcal{B}|)$ term. Moving to the blocked structure and setting

$s_{\max} = \lceil 1/\gamma \rceil$ (as was done in [14]), the output alphabets grow exponentially with the size of the block and the logarithmic term acquires a $1/\gamma$ scaling. In contrast, the scaling of the derivative of the min-tradeoff function is found to be independent of the block size. Fortunately, as our error is defined for an entire block, we reduce the multiplicative factor on the total error from $\sqrt{n}$ to $\sqrt{m} \approx \sqrt{n/\bar{s}}$. As $\bar{s} \in O(1/\gamma)$, we find that the total error term now scales as $\sqrt{n/\gamma}$. By increasing the size of the blocks we have effectively redistributed the testing probability dependence evenly amongst the components of ϵ_{DFR16}.

In [23], the authors looked to amend this deficiency by strengthening the second order term in the EAT. The following short calculation looks at how the errors scale when we applying the blocking procedure to the improved EAT statement. Recall the error terms

$$\epsilon_V^R := \frac{\beta \ln 2}{2} \left(\log\left(2|\mathcal{AB}|^2 + 1\right) + \sqrt{\text{Var}[f|_\Gamma] + 2} \right)^2, \tag{60}$$

$$\epsilon_K^R := \frac{\beta^2}{6(1-\beta)^3 \ln 2} 2^{\beta(\log|\mathcal{AB}| + \text{Max}[f] - \text{Min}[f|_\Gamma])} \ln^3\left(2^{\log|\mathcal{AB}| + \text{Max}[f] - \text{Min}[f|_\Gamma]} + e^2\right) \tag{61}$$

and

$$\epsilon_\Omega^R := \frac{1}{\beta}\left(1 - 2\log(p_\Omega\, \epsilon_s)\right). \tag{62}$$

Using the explicit form of the blocked min-tradeoff functions Lemma C.2, we can calculate the asymptotic growth of the error terms as $s_{\max} \to \infty$, $\gamma \to 0$ and $m \approx n^R/\bar{s}$. In particular, we find

$$\begin{aligned} m \cdot \epsilon_V^B &\leq \frac{\beta m \ln 2}{2} \left(\log\left(2|\mathcal{AB}|^{2s_{\max}} + 1\right) + \sqrt{\frac{(1-\gamma)^2 \bar{s} B_{\boldsymbol{\nu}}^2 (\lambda_{\max} - \lambda_{\min})^2}{\gamma} + 2} \right)^2 \\ &= O(\beta n s_{\max}) + O(\beta n/\gamma), \end{aligned} \tag{63}$$

$$\begin{aligned} m \cdot \epsilon_K^B &\leq \frac{m\beta^2}{6(1-\beta)^3 \ln 2} 2^{\beta(\log|\mathcal{AB}|^{s_{\max}} + (1-\gamma)\bar{s} B_{\boldsymbol{\nu}}(\lambda_{\max} - \lambda_{\min}))} \ln^3\left(2^{\log|\mathcal{AB}|^{s_{\max}} + (1-\gamma)\bar{s} B_{\boldsymbol{\nu}}(\lambda_{\max} - \lambda_{\min})} + e^2\right) \\ &= \beta^2 2^{O(\beta s_{\max})} O(n s_{\max}^2), \end{aligned} \tag{64}$$

$$\epsilon_\Omega^B = O(1/\beta), \tag{65}$$

and therefore the total error scales as

$$\epsilon_{\text{DF18}}^B = O\left(\beta n s_{\max} + \frac{\beta n}{\gamma} + \beta^2 n s_{\max}^2 2^{O(\beta s_{\max})} + \frac{1}{\beta}\right). \tag{66}$$

In order for ϵ_K^B to have any sensible scaling, we need the exponent to grow no faster than $O(1)$. Combining this with the inverse dependence of β in ϵ_Ω^B, we would like $\beta \approx \frac{\sqrt{\gamma}}{\sqrt{n} s_{\max}}$. Such a choice results in $\epsilon_{\text{DF18}}^B \in O\left(s_{\max}\sqrt{n/\gamma}\right)$ which suggests that indeed, the blocking procedure is no longer advantageous when used in conjunction with the improved second order statement.

A comparison between the expansion rates obtained when using the improved second order statement [23] and the blocked variant of the original EAT are presented in Fig. 8. The faster convergence to the asymptotic rate is indicative of the new EAT statement's strength.

D Conic program duality

In this section we outline the duality statements for conic programs, introduce the alternative form of dual that we use in this paper and show that it has the required properties to be considered a dual.

Definition D.1: A *cone* is a set $\mathcal{K} \subseteq \mathbb{R}^n$ with the property that if $x \in \mathcal{K}$ then $\lambda x \in \mathcal{K}$ for all $\lambda \geq 0$. A cone is *pointed* if $\mathcal{K} \cap (-\mathcal{K}) = \emptyset$.

Definition D.2: Given a cone $\mathcal{K}$, its *dual cone* is the set $\mathcal{K}^* \subseteq \mathbb{R}^n$ defined by the property that $y \in \mathcal{K}^*$ if and only if $\langle y, x\rangle \geq 0$ for all $x \in \mathcal{K}$, i.e., $\mathcal{K}^* = \{y : \langle y, x\rangle \geq 0 \ \forall x \in \mathcal{K}\}$.

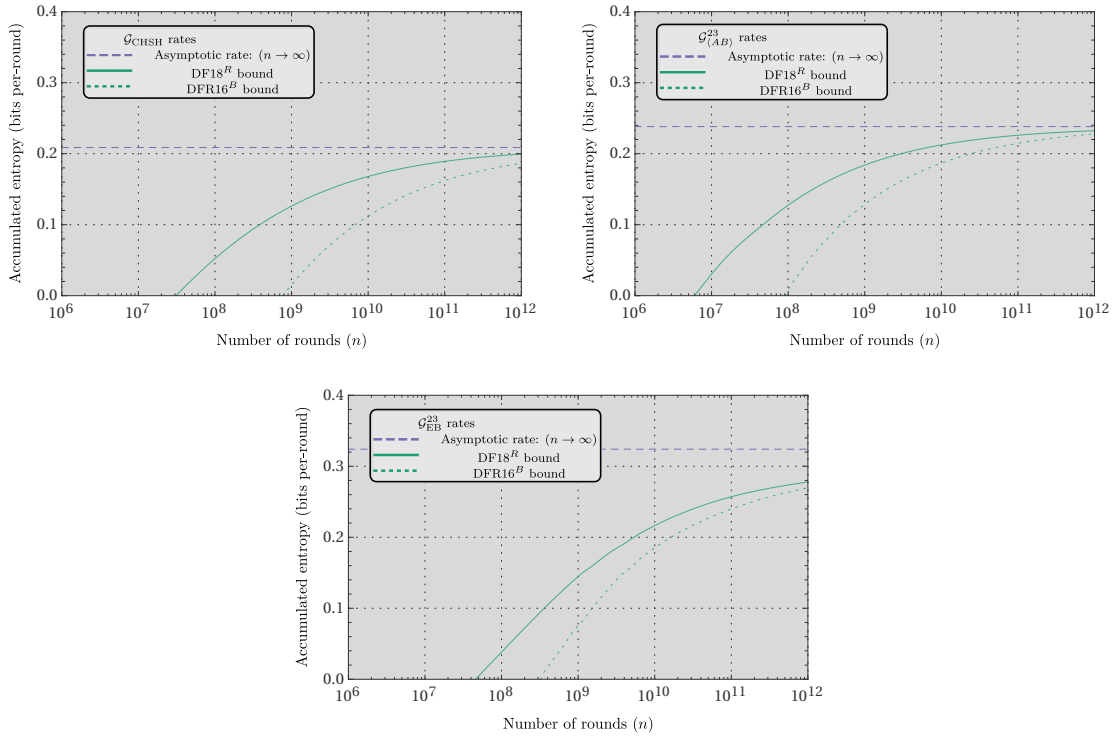


Figure 8: Comparison of the certifiable accumulation rates using the two different statements of the EAT: DFR16^B [14] and DF18^R (33). The rates were derived using the following procedure. We assumed a qubit implementation of the protocols with a detection efficiency $\eta = 0.9$, optimizing the state and measurement angles in order to maximise the asymptotic rate. Then, for each value of n an optimization of the min-tradeoff function choice was performed – for the rates calculated using (33) we also optimized the β parameter at each value of n. To ensure that we approached the asymptotic rate as n increased we set $\gamma = \delta_1 = \cdots = \delta_{|\mathcal{G}|} = n^{-1/3}$ as such a choice provides a constant completeness error across all values of n.

Definition D.3: A *proper cone* is a cone that is closed, convex, pointed and non-empty.

Definition D.4 (Dual for conic programs)**:** Let $\mathcal{K} \subseteq \mathbb{R}^n$ be a proper cone with dual $\mathcal{K}^*$, $M \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$ and consider the conic program

$$\min_{x \in \mathbb{R}^n} \langle c, x \rangle \quad \text{subj. to} \quad Mx = b,\ x \in \mathcal{K}\,.$$

The optimization

$$\max_{y \in \mathbb{R}^m, z \in \mathbb{R}^n} \langle b, y \rangle \quad \text{subj. to} \quad c = z + M^T y,\ z \in \mathcal{K}^*$$

is the dual program.

Note that this is a conic program over $\mathcal{K}^*$, the dual cone to $\mathcal{K}$.

The following two Lemmas are standard results (see, for example [71])

Lemma D.1 (Weak duality)**:** *Let P be a conic program with optimum value p^*. If the program D, dual to P has optimum d^* then $p^* \geq d^*$.*

Lemma D.2 (Strong duality)**:** *Let P be a conic program with optimum value p^* and dual D. If P is strictly feasible then $p^* = d^*$.*

Consider a family of conic programs parameterized by b, denoted $P(b)$, with optimum $p^*(b)$. Say that b is valid if there exists some $x \in \mathcal{K}$ such that $Mx = b$, and denote by $\mathcal{B}$ the set of valid b. Consider now the program $\tilde{D}(b)$ defined by

$$\max_{y \in \mathbb{R}^m} \langle b, y \rangle \quad \text{subj. to} \quad p^*(b') \geq \langle y, b' \rangle \ \ \forall b' \in \mathcal{B}$$

Lemma D.3: *If $P(b)$ has optimum $p^*(b)$ and $\tilde{D}(b)$ has optimum $\tilde{d}^*(b)$, then $\tilde{d}^*(b) \leq p^*(b)$. Furthermore, if $P(b)$ is strictly feasible, then $\tilde{d}^*(b) = p^*(b) = d^*(b)$.*

Proof. For the first part, note that the set of constraints in $\tilde{D}$ include $p^*(b) \geq \langle y, b \rangle$, so $\tilde{d}^*(b) \leq p^*(b)$.

For the second part, consider the dual problem $D(b)$ and write the constraint as $c - M^T y \in \mathcal{K}^*$. Take the inner product of $c - M^T y$ with $x^*(b')$ (the optimal argument for the primal with parameter $b' \in \mathcal{B}$) to give $\langle c, x^*(b') \rangle - \langle M^T y, x^* \rangle = p^*(b') - \langle y, Mx^* \rangle = p^*(b') - \langle y, b' \rangle$. Since $c - M^T y \in \mathcal{K}^*$, from $x^*(b') \in \mathcal{K}$ we have that $p^*(b') - \langle y, b' \rangle \geq 0$. Thus, for any $b' \in \mathcal{B}$ we have $\langle y^*(b), b' \rangle \leq p^*(b')$. The constraints in D thus imply those in $\tilde{D}$ and so $\tilde{d}^*(b) \geq d^*(b)$. If $P(b)$ is strictly feasible then by strong duality, $p^*(b) = d^*(b)$, so, combining with the first part, $\tilde{d}^*(b) = p^*(b) = d^*(b)$. □

Remark D.1: The previous lemma implies that we can think of $\tilde{D}$ as an alternative dual to P.